The European Union as a constitutional guardian of internet privacy and data protection
Hijmans, H.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU

What the European Union does and should do to make Article 16 TFEU work, by means of judicial review, legislation, supervision by independent authorities, cooperation of the authorities and external action
Promotiecommissie

Promotores:

Prof. dr. N.A.N.M. van Eijk, Universiteit van Amsterdam
Prof. dr. P.J.A. De Hert, Vrije Universiteit Brussel

Overige leden:

Prof. dr. N. Helberger, Universiteit van Amsterdam
Prof. dr. A.A.M. Schrauwen, Universiteit van Amsterdam
Prof. dr. J.E.J. Prins, Universiteit van Tilburg
Prof. dr. A. Prechal, Hof van Justitie van de Europese Unie
Prof. dr. C.B. Kuner, Vrije Universiteit Brussel
Prof. dr. S. Gutwirth, Vrije Universiteit Brussel

Faculteit der Rechtsgeleerdheid

The thesis was prepared in the Faculty of Law at the University of Amsterdam and in the Faculty Law and Criminology at the Vrije Universiteit Brussel.

Dit proefschrift is voorbereid in de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam en de Faculteit Recht en Criminologie van de Vrije Universiteit Brussel.
A foreword

An academic sabbatical for over a year resulted in this book. I recommend such a sabbatical to everyone. It was a luxury to have time and space to think. After 30 years of office life, a dramatic change of life: no specific place to go in the morning and being able to decide whether to go to the university or to stay home, to read or to write.

I could have done this earlier, but the perspective of loneliness held me back during a number of years. I had images of doing academic research in pyjamas, as a phantom in my own basement, deprived of day to day contacts with colleagues and urgencies to handle. Luckily, these images did not become reality, first, thanks to the generous offer of the Vrije Universiteit Brussels which gave me a desk where I could find refuge from my own loneliness. Second, the research itself provided me company. In some phases, the research even became a company that would never leave. It was my company in the night and woke me up in the morning. Third, and most importantly, I was not alone on this journey.

I started my sabbatical with the ambition of demonstrating that our much criticized European Union can make a difference and is capable to protect individuals in a complex society. During the period of sabattical however, much happened and the Union tumbled into a crisis. We saw, most importantly, that the Union did not manage to protect people who needed it the most, particularly those who run the risk of drowning in the Mediterranean. This background made my academic adventure even more academic, because my main argument was that Europe can make a difference and is capable to ensure individuals' fundamental rights. This trust in Europe still stands, as this book demonstrates, but it is not self-evident. We see a lack of solidarity between the European countries and a lacking belief in Europe which should not just be a market where one can pick and choose.

This book is based on combined knowledge and experience gained in different parts of my career, at various ministries with in the Dutch
government, the EU Court of Justice and in the last decade with the European Data Protection Supervisor (EDPS). It is motivated by my convictions that we need a strong state that is capable to protect its citizens, that Europe can offer solutions and that we should not give up on our European, values in a globalised world.

As said, I was not alone in this journey. My supervisors, Nico van Eijk of the University of Amsterdam and Paul De Hert of the Vrije Universiteit Brussels ensured that the research kept the right focus and would not result into an untargeted exposition of the wide variety of subjects within my field of interest. Our battles were tough, their suggestions sometimes fundamental but fully justified. For me, a session in Antwerp at Paul’s domicile in August became an urban legend. After hours of scrutiny I left, tired but also sure that in the end I would make it. It was great to rely on these two personalities, who are - in each in his own way - inspiring and who were always available.

Luckily, I could - during my research - sometimes cheat and engage in side activities, in the company of others. There were many occasions, like conferences and lectures in universities, but the best side activity was - without competition - my participation in the Privacy Bridges project, the initiative of Jacob Kohnstamm which resulted in a joint report of EU and US experts on transatlantic privacy. This project enabled me to travel twice to the US, to learn about privacy in the US from a great bunch of US colleagues and - independently of the Bridges Project - to benefit from the hospitality of Marc Rotenberg's EPIC and to do some research in EPIC’s offices. It also facilitated the contacts with Joel Reidenberg, who enriched my thesis in a few transatlantic skypes.

Others advised me at regular moments on my research. Christopher Kuner provided me with wisdom and literature, but moreover with companionship, at the numerous times we met at the VUB and discussed our common interests. Sacha Prechal used the little spare time the Court of Justice left her to help me enhance the quality of my work from the perspective of EU law. Herke Kranenborg criticized big pieces of my work in his typical Dutch style and forced me to improve. Frederik Borgesius answered numerous small questions. Stewart Watson meticulously read all texts, as the perfect Anglophone EU
lawyer. The support of Soren Schonberg confirmed that I was on the right track. When I lacked confidence, I could turn to Constance Vieco, a continuous source of inspiration in times of doubt.

In Peter Hustinx I found one of the strongest supporters of my project. Although he stayed on a distance, I felt fully reassured by the warm attention he gave me. And, although I hope that everyone likes my book, I especially hope for Peter’s approval. On a further distance, I also felt reassured by the genuine involvement of Corien Prins.

A word of thanks goes to the European Data Protection Supervisor, Giovanni Buttarelli, for giving me this opportunity and to have a break from office duties and to the fantastic EDPS colleagues I have at the EDPS, with Chris Docksey as director, to the VUB-colleagues of LSTS for giving me a temporary home and to the IVIR-colleagues in Amsterdam, for being helpful in the - too - few times I passed by.

This academic episode also fits within my personal background. Both my parents spent most of their professional lives in academia and they always stimulated me to follow their path. For a long time, this was precisely the reason not to envisage an academic career or to write a doctorate thesis. Yet, at this mature age, I changed my mind and I am happy that my father is still around to see the result of my work and to see how this makes him happy. I am sure that I would have made my mother extremely proud when she could realise that I succeeded in what determined much of her life, academic research.

Life goes on, and in recent years I not only enjoyed the continuing friendship of my old circle of friends, but also the warmth of my own loving family. To you, Zeta, my big love, and to my daughters Nina, Sophie and Nikki, who make me on my turn proud, I dedicate this book. I think I did not make you suffer too much during the writing process. I did not become the phantom in the basement, I hope, although you had to deal with some bad moods now and then. The times we spend together makes life even more wonderful.

Hielke Hijmans

Brussels, 7 January 2016
Contents

Foreword .................................................................................................................................................. 3

Chapter 1. Introduction ............................................................................................................................. 13
  1. Trigger of this Study: A Perceived Loss of Control ................................................................. 13
  2. A First Outline of Article 16 TFEU ......................................................................................... 15
  3. Research Question and the Study’s Chapters ....................................................................... 18
  4. Methodology ............................................................................................................................... 22
  5. Further Limitations ..................................................................................................................... 25
  6. Terminology ............................................................................................................................... 26

Chapter 2. Privacy and Data Protection as Values of the EU that matter, also in the Information Society ................................................................................................................................... 28
  1. Introduction ............................................................................................................................... 28
  2. Privacy and Data Protection as Part of an EU based on Values: a General Design .......... 29
  3. Privacy and Data Protection as Constitutional Values that matter, also on the Internet ....... 31
  4. Ambitions of the EU in promoting Democracy: Democracy requires a Free Internet, but not an Unprotected Internet ............................................................................................................. 34
  5. Ambitions of the EU in promoting the Rule of Law: how to ensure Effective Privacy and Data Protection on the Internet under the Rule of Law ............................................................. 36
  6. Ambitions of the EU in promoting Fundamental Rights: understanding the Context of Privacy and Data Protection and the Internet under EU law ................................................................. 41
  7. Fundamental Rights Protection against Private Parties acquires a new Dimension on the Internet, particularly for Privacy and Data Protection .................................................................................. 43
  8. The Right to Privacy, a Broad and Dynamic Concept on the Internet extending to the Public Sphere ............................................................................................................................................... 47
  9. Understanding the Nature of the Right to Privacy through four types of Qualified Interests: Information use by Governments, Health, Vulnerable Groups and Reputation ...................................................................................... 50
  10. Historical Development of the Right to Data Protection, starting as a Response to Technological Developments .................................................................................................................. 54
  11. The Right to Data Protection: a Claim based on Fairness providing Safeguards where Personal Data are processed ............................................................................................................... 59
  12. Data Protection as ‘Rules of the Game’ or ‘a System of Checks and Balances’ ............... 63
  13. Privacy and Data Protection: two Sides of the same Coin ..................................................... 66
  14. A Proposal for a Solution considering both Fundamental Rights as Part of one System ................................................................................................................................................................. 71
  15. Conclusions .................................................................................................................................. 72
Chapter 3. Internet and Loss of Control in an Era of Big Data and Mass Surveillance ..........76
1. Introduction ..................................................................................................................76
2. A General Design of the Internet and the Loss of Control over Personal Data .......77
3. The Internet as a Single Unfragmented Space with a Loose Governance Structure ....79
4. At the Core of the Internet, Networked Societies and Globalisation: Is Fragmentation a Threat? .........................................................................................................................83
5. The Internet in terms of Freedom and Powers: Is there a Shift from Freedom to Power? 88
6. Big Data justifies a Qualitative Shift in Thinking .........................................................93
7. People can no longer evade Surveillance through Electronic Means ......................97
8. No Strict Distinction between Surveillance by the State and by the Private Sector...102
9. The Perspective of the EU and the Member States: What is changing? ..................105
10. Introductory Ideas on How the EU and its Member States could regain Control...110
11. Conclusions ................................................................................................................112

Chapter 4. The Mandate of the EU under Article 16 TFEU and the Perspectives of Legitimacy and Effectiveness ...............................................................115
1. Introduction ..................................................................................................................115
2. A General Design of the Mandate under Article 16 TFEU: The Member States are Important Actors ...........................................................................................................116
3. A First Specification of the Mandate under Article 16 TFEU: Broad Powers of the EU, but a Shared Competence, and an Outline of the Three Tasks ...........................................119
4. The Exercise of the Mandate under Article 16 TFEU should comply with the Principles of Subsidiarity and Proportionality .................................................................124
5. Security Agencies could be covered by EU Data Protection despite the Limitations to EU Competence in respect of National Identities, National Security and Cultural Differences ..........................126
6. Further Limitations due to the EU’s Organisational Structure: Decentralised Implementation ........................................................................................................................132
7. Enforcement and the Organisation of Judicial Protection are normally Tasks of the Member States ..................................................................................................................135
8. Democratic Legitimacy of EU Action under Article 16 TFEU: A Prerequisite for Trust 137
9. The EU and its Citizens: The Concept of EU Citizenship contributes to the Legitimacy of the EU’s role under Article 16 TFEU ........................................................................140
10. Four Arguments Relating to a Lack of Legitimacy of EU Action ..............................143
11. The Background According to Weiler: The Crisis of Social Legitimacy ...............147
12. The Legitimacy of EU Action in Relation to the Member States: A Broad Mandate in a Pluralist Legal Context ..........................................................................................149
13. Primacy is Potentially in Conflict with the Protection of Fundamental Rights by the Member States ...........................................................................................................151
Chapter 5. Understanding and Assessing the Contribution of the CJEU to the Mandate under Article 16 TFEU

1. Introduction .................................................................................................................. 165
2. The General Design on The Task of the CJEU under Article 16 TFEU: How to cope with the Remarkable Features of this Provision? .................................................................................................................. 166
3. The Institutional Role of the CJEU in the Constitutional Order of the EU .......... 168
4. The Legitimacy of the CJEU: Compensating for the Presumed Democratic Deficit of the EU .................................................................................................................................................................. 172
5. Until the Lisbon Treaty: Emergence of Fundamental Rights in the EU Legal Order 176
7. The Test under the Charter is Strict and considers a Number of Factors ........... 186
8. The Notion of Fundamental Rights: Different Methods of defining Fundamental Rights are useful for understanding Fundamental Rights ........................................................................................................ 189
9. Distinctions between Fundamental Rights on the Internet: Towards a Simple Taxonomy .................................................................................................................................................................. 193
10. The CJEU takes a Strict Approach on Privacy and Data Protection, particularly when balancing with other Fundamental Rights, and with the Objective of Security ...... 197
11. Case Law of the US Supreme Court: Balancing with Free Speech and Security ... 200
12. Article 11 Charter on Freedom of Expression and Information: An Intensified Link with Privacy and Data Protection ....................................................................................................................... 203
13. Google Spain and Google Inc. restores a Balance, but raises Questions of Legitimacy .................................................................................................................................................................. 206
15. Article 17 Charter on the Right to Property and Intellectual Property: Do these Rights represent Essential Values in a Democratic Society? .................................................................................................. 212
17. The Contribution of the CJEU, with a Focus on Digital Rights Ireland and Seitlinger 219
18. The CJEU also promotes Integration and acts as an Umpire where Other Public Interests or Other Governmental Actors have an Impact on the Exercise of Article 16(1) TFEU 223
19. Conclusions .................................................................................................................. 227

Chapter 6. Understanding the Scope and Limits of the EU Legislator’s Contribution to the Mandate under Article 16 TFEU .............................................................................................................. 231
1. Introduction ........................................................................................................................................... 231
3. The EU Legislator’s Institutional Role, Institutional Balance and the Contributions of the European Parliament, the Council and the Commission .................................................. 238
4. Involving Other Stakeholders: Member States, Private Sector and Civil Society .. 243
5. A Comparison with the Similar, but not Equal Mandate of the EU Legislator under Articles 18 and 19 TFEU on Equal Treatment and Non-Discrimination .............................. 245
6. Elements of Privacy and Data Protection where Member States should exercise Competence: Five Categories ...................................................................................................... 248
7. The EU Legislator’s Mandate and its Interfaces with Competences of the EU and the Member States in Related Areas ................................................................. 250
8. Security: An Area where the EU and the Member States have Significant Competence 254
9. Synergies with Public Interests relating to the Internal Market: The Economic Dimension of Privacy and Data Protection .................................................................................. 257
10. Two Illustrations for Synergies: The Legal Frameworks for Electronic Communications and Consumer Protection .......................................................................................... 261
11. Competition Law, a Specific Challenge for Creating Synergies .................................... 266
12. Privacy Rules in the US: An Introduction to the Importance of Multi-Stakeholder Solutions ................................................................................................................................. 269
13. Effectiveness and Conditions for Good Legislation: Engaging the Private Sector 274
14. Accountability as an Overarching Solution for delivering Privacy and Data Protection ................................................................................................................................. 277
15. Conclusions ........................................................................................................................................ 281

Chapter 7. Understanding the Role of Independent, Effective and Accountable DPAs: New Branches of Government in between the Union and the Member States ............................... 285
1. Introduction ........................................................................................................................................... 285
2. The General Design of the DPAs: Expert Bodies with Constitutional Status and with Importance in the Information Society ........................................................................... 287
3. The Institutional Background: Six Reasons for the Existence of DPAs .................................. 289
4. The Competences of DPAs: A Variety of Roles ................................................................................. 292
5. Enforcement in the US: An Alternative System with a Strong Role for the FTC in Consumer Privacy .................................................................................................................. 297
6. The DPAs as a New Branch of Government: Non-Majoritarian Expert Bodies, Different but Similar to EU Agencies .................................................................................................. 299
8. EU Agencies and DPAs are Expert Bodies with a Hybrid Position in between the EU and National Levels .............................................................................................................. 309
9. Independence of DPAs under the Case Law of the CJEU: A Strong Requirement ... 312
10. Independence of DPAs: An Analysis .............................................................................................. 317
11. Effectiveness of DPAs: A Presumed Lack of Effectiveness and the Struggle for Resources .......................................................... 322
12. Effective Powers of DPAs, Proximity and the Developing Information Society ... 326
13. DPAs are Accountable to the Judiciary and Not Totally Free from Parliamentary Influence ................................................. 330
14. Democratic Accountability: Independence should Not mean that Expert Bodies act in a Non-Controllable and Arbitrary Manner ........................................ 332
15. Conclusions and a Model for Good Governance by DPAs ........................................ 336

Chapter 8. Understanding the Role of Cooperation Mechanisms of DPAs: Towards a Layered Model of Horizontal Cooperation between DPAs, a Structured Network of DPAs and a European DPA .................................................. 341

1. Introduction ............................................................................. 341
2. A General Design of DPAs Cooperating with Each Other and in Composite Administrations or Trans-Governmental Networks........................................ 342
3. Cross-Border Enforcement and Mutual Cooperation between DPAs: The State of Play 346
4. Institutional Arrangements: Article 29 Working Party and Other Mechanisms for Institutional Cooperation between DPAs................................................................. 349
5. Two Main Novelties in the Proposed GDPR: A One-Stop Shop Mechanism and a Consistency Mechanism .............................................................. 354
6. Experience in a Related Area: Governance in Electronic Communications through a Network of Authorities with a Task for BEREC to ensure Consistent Application............. 359
7. Cooperation between DPAs in a Composite Administration, against the Background of Developing EU Administrative Law .................................................. 362
8. Three Models to Organise Cooperation between DPAs, against the Background of the Proposed GDPR .......................................................... 368
9. The First Cooperation Layer: Horizontal Cooperation between DPAs .................. 370
10. The Second Cooperation Layer: A Structured Network of DPAs, taking the Article 29 Working Party as an Inspiration to move ahead .................................. 373
11. The Third Layer where Independence must be Ensured: Cooperation within a European DPA .............................................................................. 380
12. Cooperation between DPAs: Ensuring Independence, Effectiveness and Accountability of DPAs and the Cooperation Mechanisms, a Final Assessment and a Proposal ............................................................... 385
13. Conclusions ............................................................................ 390

Chapter 9. Understanding the EU Mandate under Article 16 TFEU in the External Domain: Towards a Mix of Unilateral, Bilateral and Multilateral Strategies ........................................ 395

1. Introduction ............................................................................. 395
2. A General Design of EU Data Protection on a Global Internet and the Relationship with Third Countries and International Organisations ........................................ 396
3. The Institutional Component of EU Privacy and Data Protection in the External Domain, focusing on the DPAs and their Cooperation..........................................................398
4. The EU and Third Countries, particularly the US: A Difference in Approach ........401
5. Two of the Most Relevant International Organisations: The United Nations do Not play a Prominent Role and the OECD underlines the Free Flow of Information........405
6. The Closest Ally, the Council of Europe: The Inspiration for EU Privacy and Data Protection, but Institutionally Difficult.................................................................408
7. A Pluralist Legal Context in the External Domain: The Relation between EU law and International law .................................................................................................................................411
8. Primacy of International Law, Subject to the Specific Characteristics and the Autonomy of EU Law........................................................................................................415
9. Jurisdictional Issues: Public International Law and the Internet .........................417
10. Jurisdiction Should be Based on a Meaningful Link with the Protection of Individuals in the EU: The Effect of an Act on the Internet on Individuals residing in a Jurisdiction.........................................................................................................................422
11. Articles 3(5) and 21 TFEU as the Starting Point for EU Action on the International Scene in Privacy and Data Protection........................................................................425
12. Unilateral Strategy: A Potentially Successful Approach ..................................427
13. Bilateral Strategy: Joining Forces with Like-minded Jurisdictions such as the US 430
15. The Meaning of the Three Strategies for the CJEU: Google Spain as an Illustration of the Unilateral Strategy under Article 16 TFEU ..................................................................435
16. The Meaning of the Three Strategies for the EU legislator: Giving Wide External Effect with the Unilateral Strategy as a Composing Element..........................438
17. The Meaning of the Three Strategies for the DPAs and the Cooperation between them: Extending Cooperation to Authorities in Third Countries.................................442
18. Conclusions .........................................................................................................445

Chapter 10. Making Article 16 TFEU Work: Analysis, Conclusions and an Analytical Grid ....450
1. Introduction ...........................................................................................................450
2. General Design of Article 16 TFEU: Recalling the Main Challenges and the Outline of the Governance under this Provision .................................................................451
3. The Analytical Grid for the Exercise of the Mandate under Article 16 TFEU and for the Contributions to this Mandate ..........................................................................................455
4. The Contribution of Article 16 TFEU to Legitimate and Effective Privacy and Data Protection on the Internet: An Appropriate Mandate is provided .........................................................459
5. The CJEU interprets the Law in Cases brought before it and acts as Constitutional Court.................................................................................................................................463
6. The European Parliament and the Council lay down the Rules, whilst Respecting the Role of the Member States under Article 16(2) TFEU ........................................................................469
7. Independent DPAs exercise Control as Expert Bodies with Full Independence, but are Not Exempted from Democratic Accountability ................................................................. 475
8. Cooperation as an Element of Control, with a Layered Structure of Cooperation Mechanisms .................................................................................................................. 480
9. External EU Action on the Internet: Solving Conflicting Jurisdictional Claims and Substantive Divergences, with a Powerful EU in the International Domain ........................................ 485
10. The Prospect of a GDPR .................................................................................................................. 490
11. Final Conclusions ................................................................................................................................ 496

SHORT SUMMARY ..................................................................................................................................... 499
KORTE SAMENVATTING ........................................................................................................................ 505
Chapter 1. Introduction

1. Trigger of this Study: A Perceived Loss of Control

The study was triggered by a perceived loss of control of governments over societal developments, due to globalisation and technological developments, which inhibit the effective protection of essential values in democratic societies.

Three examples illustrate that it is not a matter of course that European governments and EU institutions are able, in a global internet environment, to uphold and promote their values and to effectively ensure the protection European residents are entitled to. The Snowden revelations concerning mass surveillance by the National Security Agency of the United States and other governmental agencies, also in the European Union, are the first example. Snowden bears witness of massive access of governments to personal data, also where data are in the hands of private companies, in a non-transparent manner, and of a lack of overview within democratic bodies of what is actually happening.

The second example relates to the evolving era of big data, implying a shift of power to the big internet companies that hold large amounts of personal data. To illustrate the broad phenomenon of big data, we refer to the offering of ‘free’ services by search engines and social networking platforms where individuals pay with their personal data. These personal data are used for behavioural targeting, but also for combining the data for any other services and purposes. The enforcement actions by data protection authorities in the EU against, in particular, Google and Facebook show the difficulty of having control over the privacy policies used by these companies, whereas at the same time our societies become more dependent on the services of these companies. This is most clearly the case for Google, which has a share of more than 90% in the EU search engines market. The case of Facebook shows that this company, with over 1.4 billion users, combines data from a wide variety of sources, such as data originating from Whatsapp and Instagram (companies owned by Facebook), and

---

1 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State, Metropolitan Books/Henry Holt (NY).
4 Federico Ferretti, “Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?”, CMLR 51, pp. 843–868, at 864.
5 See, e.g., Chapter 8 of this study.
7 As reported by CEO Mark Zuckerberg in July 2015, see: http://versm.com/facebook-now-has-over-1-4-billion-monthly-active-users/.
from data brokers.\(^8\) In both the Google and Facebook cases, we face a lack of overview within oversight bodies as to what is actually happening, and how to keep control.

Other important factors making control over internet developments more difficult are the network structure and global nature of the internet, which does not respect physical borders of states (or the European Union), as well as the loose way in which the internet is governed, with a limited influence of governments.

The third example illustrates the resilience of the fundamental rights protection under the rule of law in the European Union and its significance for regaining trust in the Union as an actor defending the interests of its citizens. On 6 October 2015, only weeks before finalising this research, the Court of Justice of the European Union delivered its ruling in *Schrems*.\(^9\) The case was instigated by a European citizen, Mr. Schrems, who challenged the collection by Facebook of large quantities of personal data about him and who, by doing so, paved the way for a landmark decision of the European Court of Justice. The Court concluded that the 15-year-old Safe Harbour decision of the European Commission\(^10\) was invalid, based on a reasoning in which the wide access by United States authorities to personal data played an essential role.\(^11\)

The ruling brings together a number of the factors that triggered this study. The case is a clear demonstration of the difficulties of enforcement of EU data protection law by national data protection authorities vis-à-vis the big internet companies, *in casu* Facebook. The Court’s ruling also demonstrates that the EU framework provides for a system of checks and balances, where protection can be provided and where the European Union can make a difference. This does not mean that this study embraces all the aspects of the ruling, but the fact that this ruling could be given is a positive achievement of the Union’s legal framework.

In short, the perceived loss of control could reduce trust in national governments\(^12\) and in the European Union.\(^13\) In this scenario of loss of control, the Union would no longer be an actor defending the interests of its citizens, thus confirming the points of view of those who express a general scepticism on the Union. This is a general concern, as apparent from the *Schrems* case and as also recognised by the European Commission, and it emphasises that the Union must restore the confidence of citizens and businesses in the Union’s ability to deliver.\(^14\)

---

\(^8\) As reported in 2015 by Brendan Van Alsenoy a.o. in their report “From social media service to advertising network, A critical analysis of Facebooks Revised Policies and Terms, at 33-35.


\(^11\) See, e.g., para. 90 of the ruling.

\(^12\) According to the OECD only 40% of the citizens in OECD countries trust their government (2012), see: http://www.oecd.org/gov/trust-in-government.htm.


\(^14\) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation for better results - An EU agenda, COM(2015) 215 final, at 3.
2. A First Outline of Article 16 TFEU

The EU mandate under Article 16 TFEU to ensure privacy and data protection

Privacy and data protection are essential values in democratic societies, which are subject to the rule of law. The Treaties have granted the European Union a widely formulated role in ensuring effective protection of these fundamental rights of the individual by means of judicial review, legislation and supervision by independent authorities. Hence, the imperative of protection is laid down at the constitutional level, empowering the Union to play its role as a constitutional guardian of these two fundamental rights.

More precisely, Article 16 TFEU, read in connection with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, lays down the tasks of the Union in relation to privacy and data protection as fundamental rights of individuals. Article 16(1) TFEU and Articles 7 and 8 Charter specify the right to data protection, which the Union should guarantee ultimately under control of the Court of Justice. Article 16(2) TFEU empowers the EU legislator to set rules on data protection, and, finally, control should be ensured by independent authorities, according to Article 16(2) TFEU and Article 8(3) Charter.

Article 16 TFEU gives the European Union a specific mandate to ensure data protection, in addition to the general responsibility of the Union – and of the Member States when they act within the scope of EU law – to respect the fundamental rights laid down in the Charter. The Charter determines that where the Union acts, fundamental rights should be respected. Article 16 TFEU lays down that the Union shall act in order to ensure the fundamental right to data protection.

The mandate under Article 16 TFEU is broadly formulated and gives the European Union – in principle – the power to act and to make a difference. This is an area where the Union can act successfully, by addressing a problem with a global scale and that is technologically difficult.

This specific mandate of the European Union in respect of privacy and data protection is the subject of this study. The study will analyse the contributions of the specific actors and roles within the EU framework: the judiciary, the EU legislator, the independent supervisory authorities, the cooperation mechanisms of these authorities, as well as the Union as an actor in the external domain. The legitimacy and effectiveness of the Union and of the operation of the actors and their roles within the EU framework are important perspectives in this analysis.

Legitimacy and effectiveness as prerequisites for trust

Legitimacy and effectiveness are important notions in this study, since the study is based on the presumption that, in order to be successful, the exercise of the EU mandate should be
legitimate as well as effective. These two requirements are essentially different, although there is a certain overlap.

In relation to the governance of data protection, legitimacy means ensuring that there is some degree of accountability towards political institutions\textsuperscript{15} in the performance of the various roles under Article 16 TFEU. The exercise of this mandate by the European Union should be democratically legitimised, with respect of the principle of democracy and actors operating within the democratic structures, and in compliance with the rule of law and with a full system of legal protection. In the specific context of external EU action, legitimacy has an additional element, since in the external domain it is also determined by – possibly conflicting – legitimate claims of third countries and international organisations.

Effectiveness is a general principle of EU law and must ensure that adequate effect is given to EU law.\textsuperscript{16} This principle encompasses the effectiveness of judicial protection of individuals, the need for Member States to uphold the primacy of EU law vis-à-vis national law, and the effectiveness of procedures and sanctions.\textsuperscript{17} These three strands in the case law of the Court of Justice of the European Union are all relevant for the EU mandate under Article 16 TFEU.\textsuperscript{18} This study specifies the general principle of effectiveness for the governance of privacy and data protection as ensuring protection by bridging the gap between principles and practice.\textsuperscript{19}

As this study will explain, effectiveness can also be seen as an element of legitimacy. This is referred to as ‘output legitimacy’. The study takes the view that output legitimacy is not sufficient for trust; democratic legitimacy (or ‘input legitimacy’) is also required.

Legitimacy and effectiveness are essential in order to ensure – or, where necessary, regain – citizens’ trust in the ability of the European Union to deliver in the area of privacy and data protection. Trust – or confidence\textsuperscript{20} – is a term that is often used in various contexts to express the importance of privacy and data protection as factors enhancing trust in the information society.\textsuperscript{21} Trust has many connotations\textsuperscript{22} and is used in this study mainly in the sense of a belief in the competence of the Union and other actors to deliver protection.\textsuperscript{23}

\textsuperscript{15} As will be explained in Chapter 7, in relation to the CJEU case law on the independence of the data protection authorities.


\textsuperscript{17} For an elaboration, see: Koen Lenaerts, Ignace Maselis and Kathleen Gutman 2014, EU Procedural Law, Oxford University Press, at 4.05.

\textsuperscript{18} See mainly Chapter 4.


\textsuperscript{20} The term used by Eurostat (2014). See weblink in footnote 13.

\textsuperscript{21} E.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final, at 2.3; European Data Protection Supervisor, Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU".
This study emphasises the legitimacy and the effectiveness of the EU mandate in ensuring privacy and data protection on the internet. Not only does the emphasis on these two aspects provide a wider background to this specific role of the European Union, it also serves to better understand and circumscribe this role. Still, the purpose of this study even goes beyond that: its analysis and conclusions may also provide answers to questions relating to the legitimacy and effectiveness of EU action outside the areas of privacy and data protection and outside the internet context. More specifically, the model of independent data protection authorities may also prove to be useful in other areas of law.

The study’s background

The analysis in this study is made against a background in which: (a) there is no communis opinio on the role of privacy and data protection in an information society; (b) the control of governments over privacy and data protection on the internet is becoming increasingly complicated, with big data and mass surveillance as concrete illustrations; (c) governments are increasingly relying on multi-level governance, involving other actors from the private and public sectors in governance actions; (d) privacy and data protection cannot be seen in isolation from, but instead need to be balanced against other societal values; (e) the competence of the European Union in relation to fundamental rights is not undisputed, and is in any event a competence shared with Member States; (f) independent authorities have been created operating as expert bodies complementing the trias politica and the constitutional framework of the EU Treaties; (g) the cooperation between these authorities should be considered a conditio sine qua non for the effective protection of individuals; and (h) the external effect of EU action can trigger conflicting jurisdictional claims by third countries and international organisations. These eight background elements will be consecutively elaborated in the following eight chapters.

Another – dynamic – element of the background was the ongoing review of the EU framework for data protection and, more particularly, the legislative procedure relating to the proposed General Data Protection Regulation. This reform will obviously have a huge impact on the exercise of the European Union’s role as a constitutional guardian of privacy and data protection on the internet. The reform will affect the judicial review in this area and determine to a large extent how the EU legislator gives effect to the mandate under Article 16 TFEU, whereas it will also imply fundamental changes to the supervision by independent authorities. However, the reform is not the essence of the study’s analysis as the subject of this study is Article 16 TFEU, not the present or future legislative framework. It should also emphasised that the reform was ongoing during the writing of this study, with uncertain

22 “Trust is a concept that is fundamental and disparate, intuitive and indescribable”, as Lee Shaker formulates it in his paper; Lee Shaker, “In Google we trust: Information integrity in the digital age”, First Monday, Vol. 11, No. 4, 3 April 2006.


24 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.
outcomes as to crucial elements. The provisional outcome of the negotiations in a consolidated text of 15 December 2015\(^{25}\) takes away many uncertainties, but does not affect the findings of this study.

The study focuses on the specific actors and roles within the EU framework for data protection: the judiciary, the EU legislator, the independent data protection authorities, the cooperation mechanisms of these authorities, and the EU external action. The European Commission obviously plays an important role within this framework, as the title of this study underlines. The Commission's task under Article 17 TEU is usually characterised as being the “guardian of the Treaties”.\(^{26}\) Because of this task, the Commission is involved in judicial control, legislation and supervision. The Commission’s role will therefore be discussed in various chapters of this study. More generally, it is the Commission’s use of its powers under the Treaties that connects the dots and facilitates that the various actors contribute to the mandate of the EU under Article 16 TFEU in an effective and legitimate manner.

3. **Research Question and the Study’s Chapters**

The research question is formulated as follows.

How does the constitutional mandate under Article 16 TFEU contribute to legitimate and effective privacy and data protection on the internet and what does and should the European Union do to make Article 16 TFEU work, through judicial review, legislation and control by (cooperating) independent authorities, taking into account that the mandate has external effect?

The research question has a normative nature. Not only does it result in a description of the mandate under Article 16 TFEU and the contributions of the actors and roles in the exercise of the mandate, but it also aims at assessing whether Article 16 TFEU enables the European Union to respond adequately to the perceived loss of control over privacy and data protection on the internet, from the perspectives of legitimacy and effectiveness. The answer to the research question subsequently provides views on what the contributions of the actors should entail.

The study discusses the various elements of this research question in separate chapters, with the following structure. Three chapters will be more general in nature and will define what is at stake: privacy and data protection are essential values in our democracies under the rule of law and require protection (Chapter 2). This protection is being challenged on the internet, changing the scale of the problem (Chapter 3). The European Union is a key player in

---


delivering protection in a legitimate and effective manner with a specific mandate under Article 16 TFEU (Chapter 4).

The subsequent chapters will take an actor- or role-based approach and analyse how the European Union has to deliver protection, by looking at the main actors within the EU framework as specified under Article 16 TFEU: the Court of Justice of the European Union (Chapter 5), the EU legislator (Chapter 6) and the independent data protection authorities (Chapter 7). The study will present the independent data protection authorities’ cooperation mechanisms, not mentioned in Article 16 TFEU, separately, based on the view that cooperation is an essential element of control and that the cooperation mechanisms have their own responsibilities for ensuring control in a cross-border context within the Union (Chapter 8). Chapter 9 will add a wider perspective: the Union acts in a global environment and its acts have effect in the international domain. External EU action raises specific questions that are often not imputable to the specific actors under Article 16 TFEU. Chapter 10 contains the analysis and conclusions.

Chapter 2 will introduce the object of protection. It will describe privacy and data protection as constitutional values that matter in our democratic societies. The internet does not change that. Privacy and data protection are essential in a European Union based on the values of democracy, the rule of law and the respect for fundamental rights.27 These values are the wider context for explaining privacy, data protection and the relationship between these two rights. The chapter will define data protection as an entitlement to fair processing of data, not as a right to prohibit personal data from being processed. It will develop the view that in an internet environment privacy and data protection are inextricably linked. In a nutshell, privacy represents the value, data protection the rules of the game.

Chapter 3 will deal with the threats to privacy and data protection resulting from the impact of the internet. The internet has created a perception of a loss of control over data flows. The chapter will describe the internet and its governance structure, the features of the internet and the development of communications on the internet that have an impact on privacy and data protection. The chapter’s focus will be on the era of big data, in which our economies are largely data-driven, as well as on mass surveillance by private companies and governments. The chapter will explain the loss of control by governments and will conclude with preliminary remarks on ways to regain control.

Chapter 4 will introduce the broad mandate of the European Union under Article 16 TFEU28 and constitute the link between the problem – the loss of control over privacy and data protection on the internet – and the solution, the specific contributions of the various actors within the Union. This mandate under Article 16 TFEU goes beyond the Union’s general mandate to respect and promote fundamental rights. The chapter will explain the broad scope

27 See Article 2 TEU.
28 Chapter 4 will start from this notion. “By tradition European countries club together when the benefits of doing so exceed the costs in lost sovereignty” (Economist, “Europe’s energy plans are a cautious step in the right direction”, 7 March 2015, at 27, on energy policy). However, this study contains nuances to the tendency that countries are really clubbing together to address privacy on the internet.
of the mandate, as well as the limitations resulting from the general structure and arrangements of the Union. The mandate should be exercised in a legitimate manner. Citizens whose fundamental rights are at stake may expect their rights to be protected, but the often quoted democratic deficit of the Union needs to be addressed. The EU mandate impinges on the protection of individuals’ fundamental rights, which is considered a core task of national governments, as well as on the duty of the Member States to ensure the security of their citizens. Where the Union acts, Member States surrender part of their sovereignty. The chapter will focus on issues of legitimacy, based on the assumption that effectiveness of protection (output legitimacy) is not sufficient to gain or maintain trust. Democratic legitimacy (or input legitimacy) is also required. A further issue that will be explored is the exercise of the data protection mandate in accordance with the principle of effectiveness.

Chapter 5 will look at the contribution of the Court of Justice of the European Union as the actor responsible for ensuring judicial protection of the fundamental rights of privacy and data protection under Article 16(1) TFEU, read in connection with Articles 7 and 8 Charter. The chapter will discuss that the Court of Justice not only has the task of resolving disputes brought before it, but also acts as the constitutional court in the Union’s legal order with a focus on the protection of the fundamental rights. The fundamental rights of privacy and data protection are inextricably linked to other fundamental rights and public interests, which deserve protection in a democratic society subject to the rule of law. This chapter will introduce the most relevant other fundamental rights and public interests and assess how the Court assumes its role in relation to privacy and data protection in connection with these other fundamental rights and public interests. Finally, the chapter will touch upon the role of the EU Court of Justice in promoting integration in the Union and as the umpire adjudicating between different competences.

Chapter 6 will analyse the contribution of the EU legislator under Article 16(2) TFEU. It will explain the characteristics of the EU legislator’s mandate and the perspectives of the players in the legislative process. These are primarily the European Parliament, the Council and the Commission, but the Member States, the private sector and civil society have a role to play as well. The chapter will compare Article 16 TFEU with the specific mandate of the European Union relating to non-discrimination. Subsequently, it will address the mandate of the EU legislator and the interfaces with the competences of the Union and the Member States in related areas. Furthermore, the study will focus on the effectiveness of the various instruments that can be adopted under Article 16 TFEU, from the perspective of the quality of legislation. The involvement of the private sector will also be addressed, including the accountability of data controllers, a key concept in modern data protection.

Chapter 7 will introduce the role of the independent supervisory authorities for data protection, based on Article 16(2) TFEU and Article 8(3) Charter. These data protection authorities (DPAs) have a complex position as national authorities operating within the national jurisdiction, yet also having a critical role as guardians of the EU mandate to safeguard privacy and data protection. This study will elaborate the constitutional position of these independent supervisory authorities, consisting of experts to whom public tasks have been delegated, in particular the sensitive task of protecting specific fundamental rights. The
DPAs will be described as a new branch of government, operating in between the Union and the Member States. The chapter will include a reflection on the similarities and differences between expert bodies in other areas of EU action. The case law of the Court of Justice of the European Union sets high standards for their independence, but also emphasises an element of legitimacy as DPAs should be accountable in a democratic society. The chapter will discuss the independence, legitimacy and effectiveness of DPAs.

Chapter 8 will specify the cooperation mechanisms between data protection authorities. Cooperation between DPAs is an essential element of their task of ensuring control, in particular on the internet. The chapter will explain that these mechanisms have an autonomous role in the control of privacy and data protection, one that is not explicitly provided for in the Treaties. The chapter will introduce the Article 29 Working Party and other mechanisms for institutional cooperation between DPAs. The General Data Protection Regulation will introduce two novelties: a one-stop shop mechanism and a consistency mechanism. The study will describe similarities with the cooperation mechanism in the related area of network governance in electronic communications. Cooperation between DPAs takes place in a composite administration and against the background of developing EU administrative law. The chapter will distinguish various models of cooperation: cooperation between the authorities, a structured network of these authorities, and the transfer of certain tasks to a European supervisory authority. These cooperation mechanisms present a further challenge to democratic legitimacy, as well as to the effectiveness of the control.

Chapter 9 will discuss a necessary complement of the EU mandate and the main actors’ contributions to this mandate: the Union’s role in the external domain. This includes the relationship with third countries and international organisations, with a focus on the United States as third country and the United Nations, the Organisation for Economic Co-operation and Development and the Council of Europe as the most relevant international organisations. The powers of the European Union are determined both by EU law and international law. External effect of internal EU law on data protection is inherent in an internet environment where the data flows are across the whole world. An external effect also arises as a consequence of the Union’s explicit choice for wide jurisdictional claims in order to achieve better protection of individuals in the Union. This all means that EU action is not confined to EU territory and may thus impinge on legitimate claims of other jurisdictions. The chapter will discuss external EU action, as well as various models for establishing jurisdiction, and explore three possible strategies – unilateral, bilateral and multilateral – for the Union to enhance protection outside its territory. The study will analyse the significance of these strategies for the main actors under Article 16 TFEU.

Chapter 10 will summarise the analysis and contain the conclusions, based on the findings of Chapters 2-9. It will also introduce an analytical grid to enhance the understanding of the Union’s mandate and the various roles within this mandate. The analytical grid is a tool for the assessment, based on the research question and its various components. Towards the end, the chapter will include a few observations on the perspectives under the General Data Protection Regulation.

---

29 See in particular Case C-518/07, Commission v Germany, EU:C:2010:125.
Protection Regulation, after its adoption and entry into force. The chapter will close with the study’s final conclusions.

4. Methodology

This is a legal study written from the perspective of EU law, particularly EU law on privacy and data protection. This focus determines the content of the study.

The perspective dealt with in this study is law. Where the study touches on technological phenomena, this is purely in order to provide a better understanding of developments in law and society, without the author claiming to have any particular technological knowledge. The same goes for other relevant academic disciplines, in particular economics and social sciences. This study draws on sources from all these disciplines for issues such as the balancing of costs and benefits of certain options\(^{30}\) and actual behaviour on the internet.\(^{31}\) Chapter 3 on the internet and loss of control will be based on a few authoritative sources, including the work of Castells.\(^{32}\)

The perspective is EU law. Other sources of law are included in the study, but not with the aim of adding a comparative law dimension to the study. Where the study mentions national law of the Member States, this is mainly by way of illustration. International law is discussed only where it has relevance within the EU jurisdiction. In a study on fundamental rights, the European Convention on Human Rights (ECHR) and the case law of the European Court of Human Rights (ECHR) in Strasbourg obviously have a special status. The focus on the relationship with the United States – as explained below – results in various references being made to US law, including case law of the US Supreme Court.

The perspective is the law on privacy and data protection. The study’s subject is Article 16 TFEU, taking the existing arrangements for data protection as a starting point. The study also refers to the reform of the EU data protection framework, with a strong focus on the proposed General Data Protection Regulation,\(^{33}\) insofar as this has added value for explaining Article 16 TFEU. An important reason for this approach is that the negotiations on this new framework were taking place when this study was being written. The outcome of these negotiations will bring crucial changes to the landscape of privacy and data protection.

\(^{30}\) As is done in a ‘law & economics’ approach.
\(^{31}\) An approach of social science.
\(^{33}\) Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. Of less importance for privacy and data protection on the internet is the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final. The reform is expected to consist of additional legal instruments, such as a new instrument for data protection within the EU institutions and bodies as announced in Article 90a of Consolidated text (outcome of the trilogue of 15/12/2015), available on http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884.#.
Taking privacy and data protection as a basis means that other areas of EU law will be addressed only if:

a. They determine the framework for issues relating to data protection and its governance;
b. They provide examples that are or may be relevant for data protection;
c. There is a reason for convergence with the area of data protection, for example, if it would make sense for regulators in another area to contribute to better data protection or if data protection authorities could or should take other public interests into account;
d. Data protection may have an interface or may collide with other fundamental rights or public interests.

The perspectives are the legitimacy and effectiveness of the governance of privacy and data protection provided by the European Union and the main actors within the Union. Legitimacy and effectiveness will be at the core of Chapter 4, which constitutes the link between the perceived loss of control over privacy and data protection on the internet, on the one hand, and the specific mandate of the Union and its various actors to address this problem, on the other hand.

The emphasis on legitimacy and effectiveness of governance also means that the substantive principles of data protection, as laid down in Article 8 Charter, in Directive 95/46 and in other instruments of EU data protection law, will not be analysed in this study, although they obviously play a role in various parts of it. The study is about governance of data protection in the European Union and addresses the substance of data protection law only insofar this relates to the choice of governance mechanisms.

The mandate of the European Union, including the exercise of the various roles under this mandate, has the following objectives:

a. Ensuring protection, through full respect of the rights to privacy and data protection and the restrictive application of exceptions and limitations;
b. Balancing with other fundamental rights and essential interests in society;
c. Managing centralisation, which is an inherent effect of the EU mandate under Article 16 TFEU and includes balancing the mandate with the competences of the Member States.

This study takes a selective approach and does not systematically discuss how the respective actors and roles deal or should deal with all three objectives. The chapters will demonstrate that the contributions of the various actors and roles raise a variety of issues. These issues are not identical for each and every actor and role, although the aspirational goals are the same: contributing to the respect of privacy and data protection. This explains the diversity in the focus of this study’s chapters:

a. Chapter 5 on the contribution of the Court of Justice of the European Union to Article 16(1) TFEU will place an emphasis on the understanding and respect of the right to data protection and the restrictive application of exceptions and limitations,
particularly by discussing the balancing with other fundamental rights and essential interests in society;

b. Chapter 6 on the contribution of the EU legislator will discuss the problem of managing centralisation, an inherent effect of the Union’s mandate under Article 16 TFEU, in connection with the competences of the Member States. It will also consider how the rights to privacy and data protection as such can best be respected through the choice of instruments;

Chapter 6 on the contribution of the EU legislator will discuss the problem of managing centralisation, an inherent effect of the Union’s mandate under Article 16 TFEU, in connection with the competences of the Member States. It will also consider how the rights to privacy and data protection as such can best be respected through the choice of instruments;

c. Chapter 7 will focus on the independent data protection authorities, as mechanisms for legitimate and effective protection. Managing centralisation is a second angle, given that these authorities operate at the intersection between Brussels and the Member States;

d. Chapter 8 will address the cooperation mechanisms of the data protection authorities, with a strong focus on managing centralisation. The difference between the cooperation mechanisms (cooperation between the DPAs, a structured network of DPAs and the transferring of certain tasks to a European supervisory authority) relates to a large extent to the degree of centralisation;

e. Chapter 9 on the external aspects of the European Union will focus on ensuring protection since the perceived loss of control over personal data is largely due to the borderless nature of the internet, with its global and ubiquitous data flows.

The analysis of the organisational aspects of the data protection authorities and their cooperation mechanisms is more profound than the analysis of these aspects of the judiciary and the legislator. The reason for this is that data protection is just one of the many tasks of the Court of Justice and of the European Parliament and the Council acting as the Union’s legislator, whereas it is the core task of the data protection authorities. Analysis of the resources of DPAs – to take an example – is relevant for this study, if only because the use of resources is important for the DPAs’ effectiveness and legitimacy. By contrast, discussing the resources of the Court of Justice and of the European Parliament and the Council clearly falls outside the scope of the study.

The research is based on assumptions on shortcomings in relation to the protection of privacy and data protection on the internet that have been widely recognised in various sources. These assumptions will not be scientifically examined, but will be used as the points of departure of the analysis.

The analysis in this study will generate a number of conclusions, all of which aim at contributing to a legitimate and effective exercise of the EU mandate in privacy and data protection, with a view to regaining trust in the capabilities of the European Union to protect and, by doing so, contribute to trust in the Union itself. These conclusions are linked, but not interdependent. Disagreement with one conclusion consequently will not affect the validity of other conclusions.
Finally, adopting a perspective based on law means that the research is largely based on the study of legal documents, such as legislative documents,\textsuperscript{34} case law, literature, policy documents and other public sources relating in some way to law. In addition, during the research discussions took place with a selection of main stakeholders. The author contributed to various seminars relating to the topic of this study. The study also benefited from the input of an Expert Seminar organised by the University of Amsterdam on 27 October 2014, at which experts from various legal disciplines discussed some main issues of this study, as well as from the author’s participation in the ‘Privacy Bridges’\textsuperscript{35} project and from a short stay at the Electronic Privacy Information Centre in Washington DC.

This study is the result of a research that was finalised on 30 October 2015. On that date, the manuscript was sent to the doctorate jury. Developments after this date are not reflected in this study.

\textbf{5. Further Limitations}

This study takes the perspective of the European Union acting as a guardian of privacy and data protection and does not elaborate on internet security. Insufficient security may be a threat to the internet as such and to the protection of personal data on the internet. This limitation of the study is in line with a distinction made in literature, whereby developments on the internet that lead to threats to privacy and developments leading to threats to security are seen as two distinctive concerns.\textsuperscript{36} In the context of this study, it suffices to keep in mind that security threats are significant as a result of the internet as a network society.\textsuperscript{37}

The study does not question the architecture of the internet, nor its governance. It just gives a description insofar as relevant for the research, and points to some likely developments in the near future.

The same goes for the state of EU integration. Any suggestions made here for better enforcement will not require Treaty changes, or at least that is not the aim of the research. A further limitation is that the study focuses on fundamental rights, but does neither extend to the procedure foreseen in Article 7 TEU for events that pose a clear risk of a serious breach of constitutional values by a Member State, nor to the EU’s accession to the European Convention of Human Rights.\textsuperscript{38}

\begin{thebibliography}{99}
\footnotesize
\item In a wide sense, on the one hand also including international treaties and national legislation and on the other hand also including soft law instruments.
\item E.g., Bruce Schneier, \textit{Data and Goliath}, (W.W. Norton & Company, 2015).
\item Unlikely to happen on the very short term, as a result of Opinion 2/13 of the Court of Justice, EU:C:2014:2475.
\end{thebibliography}
Where the study deals with external effects of EU action – which are unavoidable in relation to the internet – it focuses on the position of and relationship with the United States and does not discuss positions of other third countries.\(^{39}\) This choice is justified for the following reasons: the US represents the predominant economy on the internet; many issues relating to phenomena and developments on the internet have a US background, with mass surveillance being the most obvious example; there is interesting case law on the subject, for instance from the US Supreme Court; and the European Union and the United States share the main values on fundamental rights, even though the arrangements for protection are essentially different. This divergence of protective arrangements has been referred to as a transatlantic divide\(^{40}\) and is said to complicate the development of global solutions.\(^{41}\)

The analysis of international organisations’ activities focuses on the organisations with which the European Union, under Article 220(1) TFEU, has to establish appropriate forms of cooperation, more specifically the United Nations and, where relevant, its specialised agencies, the Council of Europe and the OECD.

### 6. Terminology

The study is based on a common understanding of the following terminology.

- Privacy and data protection are considered to be one complex of concerns and are usually addressed together in this study. However, some provisions deal only with data protection, whereas some explanations deal exclusively with privacy.
- Fundamental rights are distinguished from public interests.
- Security has various dimensions, ranging from the safeguarding of citizens’ physical security (a public interest) to the technical security of data systems (an element of data protection).
- Proportionality has a different meaning in different contexts: as a limitation of the intervention powers of the European Union pursuant to Article 5(4) TEU and as a limitation of fundamental rights pursuant to Article 52 Charter.
- Government is understood to comprise the entire public sector, consisting of the traditional *trias politica* (the executive, legislative and judiciary), as well as the independent authorities qualified as a “new branch of government”\(^{42}\).
- Multi-level governance equals multi-stakeholder solutions and includes the private sector’s involvement in governance; this is not the same as a pluralist legal order, which is about the interfaces between different governmental levels.

\(^{39}\) A good overview of the main elements of the US law and structures in this area can be found in: Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions”, Amsterdam / Cambridge, September 2015, available on: https://www.chpweb.nl/sites/default/files/atoms/files/privacy_bridges_paper.pdf. The sections on US law and structures in this study are meant to illustrate the context in which the EU operates.


\(^{42}\) See particularly Chapter 7.
Some abbreviations are used regularly throughout the study: the “Court” is usually the Court of Justice of the European Union in Luxembourg, sometimes referred to as the European Court of Justice, “Charter” is the Charter of the Fundamental Rights of the Union, “TEU” is the Treaty on European Union, “TFEU” is the Treaty on the Functioning of the European Union, “ECHR” is the European Convention on Human Rights, the “ECtHR” is the European Court of Human Rights in Strasbourg, “Convention 108” is the Council of Europe Convention on data protection, and “DPAs” are independent data protection authorities. When the term NSA is used, this refers to the National Security Agency of the United States.

Many of the examples in this study are taken from Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, referred to as “Directive 95/46”. The main legislative proposal in the area is the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), or shortly the “General Data Protection Regulation”, which is expected to result in the setting-up of a European Data Protection Board (“EDPB”), not to be confused with the European Data Protection Supervisor (“EDPS”).

---

44 OJ L 281/31.
Chapter 2. Privacy and Data Protection as Values of the EU that matter, also in the Information Society

1. Introduction

There is no *communis opinio* on the role of privacy and data protection in the information society. Our economy is driven by the use of large amounts of data. Many people benefit voluntarily from the advantages of this data-driven economy by, for instance, sharing personal information on social networks and remaining constantly connected to the internet through their mobile devices. By sharing this information they accept, at least implicitly, that they may be tracked.

This chapter analyses the object of protection: our privacy and personal data on the internet need to be protected legitimately and effectively, and EU law needs to guarantee such protection. The analysis provides elements for answering the general part of the research question, namely: “How does the constitutional mandate under Article 16 TFEU contribute to legitimate and effective privacy and data protection on the internet?” This analysis includes:

a. the general design of privacy and data protection;
b. privacy and data protection as values that matter, also on the internet;
c. the ambitions of the EU in promoting democracy, the rule of law and fundamental rights;
d. protection of fundamental rights against private parties on the internet;
e. the development of the right to privacy into a broad and dynamic concept on the internet;
f. the development of the right to data protection into a claim based on fairness;
g. privacy and data protection as two sides of the same coin and a proposal for considering both rights as part of one system.

The first objective of the chapter is to demonstrate that the respect for privacy and data protection on the internet are important for individuals and our societies, as well as for the European Union, which is based on values and has the ambition to protect these values. The second objective is to delineate the object of protection under EU law and in an internet environment.

This study takes the position that the internet poses challenges for the effectiveness of privacy and data protection, but that this does not change the need for protection of these fundamental rights in a democracy under the rule of law. Privacy and data protection remain social norms, irrespective of the fact that views in society on these values seem to be changing. Our democratic societies, under the rule of law, can function only if individuals have a certain degree of dignity and autonomy.

---

46 As explained in Section 3 of this chapter.
There is an imperative for governments to ensure that protection is given to individuals, also in the online environment. For the European Union, this imperative is laid down in the specific mandate under Article 16 TFEU. Respect for privacy and data protection is part of a European Union based on the values of democracy, the rule of law and fundamental rights.

The chapter starts in Section 2 with a general description of privacy and data protection as part of a European Union based on values. Section 3 presents arguments why privacy and data protection represent constitutional values that matter on the internet. Sections 4 and 5 explain the ambitions of the Union in terms of ensuring constitutional values of democracy and the rule of law in relation to internet privacy and data protection.

Sections 6 and 7 deal with the ambitions of the European Union in promoting fundamental rights. Section 6 discusses a few specific elements involved in fundamental rights protection so as to enable an understanding of privacy and data protection on the internet in a European Union based on values. Section 7 is dedicated to a subject that acquires a new dimension on the internet: fundamental rights protection in horizontal relations, against private parties.

In Sections 8-14 the focus becomes narrower: the sections elaborate on the precise object of protection. The right to privacy protects individuals against interference. This right has a broad scope and also extends to the public sphere (Sections 8-9). The right to data protection contains a set of rules on fair and lawful data processing, elaborated into specific obligations for organisations (‘data controllers’) and specific rights for individuals (‘data subjects’). Individuals are entitled to their data being processed fairly, but cannot prevent the processing of their data (Sections 10-12). Sections 13-14 argue in favour of a combined reading of privacy and data protection under Articles 7 and 8 Charter. Drawing a distinction between these two rights makes no longer makes sense on the internet. Section 15 contains the conclusions.

### 2. Privacy and Data Protection as Part of an EU based on Values: a General Design

Article 2, first sentence, of the Treaty on European Union reads: “The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.”

The values of democracy, the rule of law and human or – in an EU context – fundamental rights are at the basis of the existence of the European Union. Hence, privacy and data protection as fundamental rights in a developing information society are elements of the wider ambitions of the Union to promote the values laid down in Article 2 TEU.

Privacy, data protection and the ambitions of the EU in promoting its values

---

47 As illustrated by the case law of the CJEU, in particular Joined Cases C-92/09 and C-93/09, Schecke (C-92/09) and Eifert (C-93/09) v Land Hessen, EU:C:2010:662, and Case C-131/12, Google Spain and Google Inc., EU:C:2014:517.
Privacy and data protection are recognised in Article 16(1) TFEU and in Articles 7 and 8 Charter as essential elements of a European Union based on values. As this study explains, the protection of these fundamental rights should be based on the following notions: these fundamental rights are applicable in all situations, the Court of Justice’s scrutiny of the European Union is strict, and the application in horizontal situations between private parties acquires a new dimension on the internet, including a duty for the European Union to ensure protection.

The values of the European Union and its high ambitions in promoting these values are prominently laid down in primary EU law and confirmed both in policy documents of the institutions and in the case law of the Court of Justice. These sources give a clear picture of the moral role the Union seeks to play, both within its own territory and in the wider world. They reflect the aim of European integration, based on peace and democracy and initially starting off, in reaction to the Second World War, as a project focusing on economic integration, but always with higher ideals in mind.\textsuperscript{48}

In the preamble to the Treaty on European Union, the Member States (the parties to the Treaty) confirm their attachment to the principles of liberty and democracy, as well as to respect for human rights, fundamental freedoms and the rule of law. Article 2 TEU specifies this commitment. The aim of the Union is to promote these values (Article 3 TEU), which are not only of a constitutional nature,\textsuperscript{49} but are also considered universal.\textsuperscript{50}

The Treaty on European Union refers to democracy, the rule of law and fundamental rights. These three values are inextricably linked\textsuperscript{51} and fundamental to all activities of the Union. They are supposed to “underpin all aspects of the internal and external policies of the European Union.”\textsuperscript{52} Another illustration of the need to respect the values of the Union is the procedure of Article 7 TEU, which may lead to the suspension of a Member State in the event of a clear risk of a serious breach of these values, a procedure that in itself has no further relevance for this study.

This inextricable link between values is made explicit in the Treaty on European Union and, therefore, in the constitutional charter of the Union.\textsuperscript{53} The Union, being based on values, should promote not only fundamental rights, but also democracy and the rule of law. Respect for all these values is essential if EU action is to be legitimate. The Treaties not only mention these values, but also attribute a universal value to them.\textsuperscript{54} Furthermore, these values are

\textsuperscript{48} See, e.g.: Luuk van Middelaar, De passage naar Europa. Geschiedenis van een begin (published in English as: The Passage to Europe: How a Continent Became a Union), Historische Uitgeverij.
\textsuperscript{49} They have a constitutional nature since the Treaties are the basic constitutional charter of the Union, as recalled by the CJEU in its Opinion 2/13, EU:C:2014:2475, at 163.
\textsuperscript{50} Preamble and Article 21 TEU.
\textsuperscript{51} Aharon Barak, Proportionality; Constitutional Rights and their limitations (Cambridge University Press, 2012), at 2-3 and 161-162.
\textsuperscript{53} See, e.g.: Opinion 2/13, EU:C:2014:2475, at 163.
\textsuperscript{54} Preamble and Article 21 TEU.
shared by all the Member States and represent the premise of mutual trust, both among the Member States themselves and between the Member States and the Union.\(^{55}\)

That said, laying down ideals in official texts does not in itself guarantee a Union that is fully equipped and has the legitimacy needed to realise these ideals. This study explores their meaning, in practice, for privacy and data protection on the internet.

### 3. Privacy and Data Protection as Constitutional Values that matter, also on the Internet

The features of and developments of communications on the internet are changing our societies in a fundamental way.\(^6^{6}\) In addition, the views in society on the use of personal data are evolving. Wide-ranging groups of individuals – but definitely not all individuals – voluntarily share large amounts of personal information on social media. Moreover, the views are changing on the societal benefits of the use of big data, recognising that big data may significantly improve the quality of government action in a wide range of areas.\(^{57}\)

Big data is a much wider concept than personal data since the former also includes large data sets that are not related to identified or identifiable natural persons.\(^{58}\) One way to fully benefit from big data, however, is precisely through the fact that personal data, too, can be used for broad purposes. This, in turn, is difficult to align with purpose limitation, which is a basic principle of data protection.\(^{59}\) This wide use of personal data is said to have added-value for our democracies. Notions such as open data and net neutrality are relevant in this context, as is an open internet that is not regionally fragmented.\(^{60}\) The protection of the physical security of individuals may require the use of large amounts of personal information.\(^{61}\)

These examples illustrate changing views on the exercising of the rights to privacy and data protection and on intrusions of these rights. Some intrusions are perceived as annoying, while others are serious. To make things even more complicated, the perception of the nature of an intrusion is based, to a certain extent, on subjective ideas: people value the seriousness of

---


\(^{56}\) This will be elaborated in Chapter 3.


\(^{58}\) Definition of personal data in Article 2(a) of Directive 95/46. On big data, see Chapter 3.

\(^{59}\) This is laid down in Article 8 Charter, which states that personal data must be processed for specified purposes.

\(^{60}\) This is an important argument in the debate surrounding Case C-131/12, Google Spain and Google Inc., where critics point to the fact that the ruling may possibly lead to censorship of the internet if it obliges search engines to remove certain links.

\(^{61}\) A recurring issue, as illustrated by the legislative reactions to 9/11 and Charlie Hebdo and also by the Snowden revelations (see mainly Chapter 3).
privacy breaches in divergent ways, as evidenced by the massive use of personal data in business models designed to capture value from personal data for behavioural targeting of consumers. Is it a serious breach of privacy that people’s data are subsequently being used for targeted advertising without their knowledge, or is this just annoying?

This being said, the starting point of this study is that our democratic society, which is subject to the rule of law, can only function if individuals have a certain degree of autonomy and privacy. The obvious reference in literature in support of this starting point is George Orwell’s 1984. A more recent literary witness is The Circle by Dave Eggers. The main argument in this study is that all individuals, not only those involved in doing bad things, have something to hide, simply because people are entitled to do things in a private sphere that they do not want to make public. And the fact that many – though not all – people are prepared to share large parts of their private sphere online, for instance on social media, does not alter this.

In a TED Talk (2014), Glenn Greenwald convincingly argued in support of the importance of privacy and data protection in an information society generating the potential for mass surveillance of every individual. He refuted statements by leaders of big internet companies that you had better not do things if you do not want them to become public or that privacy is no longer the social norm. An example of the latter is the statement by Mark Zuckerberg, founder and CEO of Facebook, that “The rise of social networking online means that people no longer have an expectation of privacy.”

Two elements stand out: there are no good or bad people, and monitoring changes behaviour

Two elements stand out in Greenwald’s reasoning in the context of this study: there are no good or bad people, and monitoring changes behaviour. Firstly he states that one cannot divide the world into good people and bad people, with the first group consisting of people who have nothing to fear from monitoring because they have done nothing wrong, and the second group being the justifiable target of monitoring, precisely because they have done something wrong, or can reasonably be suspected or expected to do so. Secondly he explains that constant monitoring may indeed change behaviour and lead to a society where people become conformist and compliant. Human shame or embarrassment could be a reason for adapting behaviour that is legal and not harmful to others, but is not mainstream. For a

---

62 The recurring question in debates on privacy breaches is “Is this really a problem?” or, in my native Dutch tongue, “Wat is hier erg aan?”.
63 See: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on “Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”, at Section 2.
64 Dave Eggers, The Circle (McSweeney’s, 2013).
66 Statement attributed to Eric Schmidt, former CEO of Google.
67 Statement attributed to Mark Zuckerberg, founder and CEO of Facebook.
democratic society it is important to respect non-mainstream behaviour or, more specifically, behaviour by political and societal minorities.

This study does not claim that massive use of personal data, even without the knowledge of the individuals concerned, by definition leads to unjustified interference of privacy or other fundamental values in a democratic society. It does claim, however, that the arguments of Greenwald in favour of privacy and data protection are convincing. The substantive increase in the use of massive amounts of data may well affect individuals and democratic societies adversely, unless this use is accompanied by effective and legitimate rules to counterbalance the undesired effects.

These undesired effects can be summarised as lack of control over information, which hampers the autonomy of individuals, and full transparency of individuals and their behaviour, which hampers their dignity. These effects do not alter the fact that many individuals share large amounts of private information online on a voluntary basis. For these individuals, privacy may have a different or possibly less important meaning, or may even no longer be the social norm. This does not mean, however, that all individuals are no longer entitled to protection of a fundamental right, even if only a minority of them care.

The Snowden revelations are an illustration of these effects on individuals and society. Not only are people shocked by the fact that a foreign power is able to infringe their fundamental rights on a massive scale, thus adding a genuinely new dimension, but people also do not even know the scale and nature of what is really happening, and nor do governments always know this. It has even been claimed that some governments are kept unaware of surveillance activities involving their own citizens.

These effects are also the result of the evolving era of big data, implying a lack of control over information by individuals and thus shifting the power to those who hold large amounts of personal data, such as the big internet companies.

These effects are obviously not new. As will be explained below, technological developments have led to the recognition of privacy and data protection as fundamental rights and to their inclusion in primary EU law. This study argues, however, that it is the scale of intrusions into these fundamental rights that is new. And this new scale of intrusions

---

69 Autonomy and dignity are referred to in Section 8 of this chapter as the underlying values of privacy and data protection.
70 As implied by Mark Zuckerberg. See footnote 67.
72 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State (Metropolitan Books/Henry Holt (NY), 2014), at 5-6.
74 See Sections 8 and 10 below.
influences the protection that is required in a European Union based on values and operating in an effective and legitimate manner.

4. **Ambitions of the EU in promoting Democracy: Democracy requires a Free Internet, but not an Unprotected Internet**

This section discusses the European Union’s ambitions in promoting democracy in relation to privacy and data protection on the internet. Privacy and data protection are essential in a democracy for two reasons. Firstly, a democratic society cannot exist if individuals do not have the assurance of the full exercise of their fundamental rights under the rule of law. It is the respect for the rights of individuals that distinguishes a democracy from a totalitarian state. Secondly, one of the main objectives of the protection of fundamental rights is to guarantee the participation of individuals in a democratic society under the rule of law. This is the essential nature of the freedom of expression and information, enabling “expression to be given to opinions which differ from those held at an official level” and of connected rights recognised in most Western constitutions, such as the freedom of assembly and of association.

The rights to privacy and data protection also have a connection with participation in a democratic society since respect for privacy and data protection, thus preserving the autonomy of individuals, is also a prerequisite for exercising the freedom of expression. If privacy is not respected, this will have a chilling effect on individuals’ participation in a democratic society. Hence, privacy and data protection are not just fundamental rights of individuals, but are also essential for the functioning of our democratic societies.

**Democracy as guiding principle in relation to the internet**

Democracy is a guiding principle in relation to the internet in that the latter must be a sphere in which democracy flourishes. A free internet is seen as empowering individuals to share information in an unprecedented way, and hence as boosting democracy. In its proposal for a regulation concerning the European single market for electronic communications, the Commission provides for a right to participate on the internet, whereby “End-users shall be free to access and distribute information and content, run applications and use services of their choice via their internet access service.”

---

75 E.g., Aharon Barak, Proportionality: Constitutional Rights and their limitations, (Cambridge University Press, 2012); European Parliament, Directorate-General for Internal Policies, Policy Department C, Citizens’ Rights and Constitutional Affairs, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, at 12 (referred to in Chapter 3, Section 7 of this study).
77 Articles 11 and 12 Charter.
78 As explained by Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015), at 95-97. The argument of the chilling effect is also often referred to in Europe.
79 E.g., Center for Democracy and Technology, “Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age”, Discussion Draft Version 0.5, April 2011.
80 Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending
A free internet could also mean that whereas individuals are to a large extent dependent on big internet players, they may require those players themselves to act in a transparent way as a prerequisite for a free and democratic society.

The link between the internet and democracy is often made, by depicting the internet as a space where the free flow of information is promoted, that protects human rights and that fosters innovation, in short an environment where democratic values are fully respected. The European Commission even states that the internet facilitates democratic progress worldwide.

One of the justifications for restricting government intervention on the internet is the fact that states may attempt to curb the global connectivity of their citizens by censorship and other restrictions of free speech.

_A free internet does not mean an unprotected internet_

Democracy must flourish on the internet. This essentially means that governments may set conditions where necessary, but must in principle abstain from intervention. This is one of the reasons why the Commission has embraced the model of multi-stakeholder governance structures for the internet, with limited government participation. In certain situations, however, governments should also actively ensure that democratic rights are respected, and this requires active government intervention. Privacy and data protection must be guaranteed: Article 16 TFEU provides the European Union with the mandate to do so.

Moreover, the respect of democracy on the internet also requires democratic governments to protect democratic societies against threats, such as those caused by serious crime and terrorism. This may require restrictions to or limitations on the exercising of fundamental rights, insofar as such restrictions or limitations are “necessary in a democratic society”, as illustrated by the abundant case law, in particular of the European Court of Human Rights.

---

81 As will be explained in Chapter 3.


83 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance Europe's role in shaping the future of Internet Governance, COM/2014/072 final, at 2.


85 This wording is used in various articles of the ECHR.

Proportionality is the yardstick for these restrictions or limitations. Within the EU context, the case law on restrictive measures for the fight against terrorism – such as the freezing of certain individuals’ assets, thus restricting their right to property – is an example of how it can be necessary to restrict a fundamental right in a democratic society, notwithstanding the fact that the measures taken must obviously be proportional. More generally, the fight against terrorism – in particular in the period following 9/11, but equally in reaction on the tragic events in Paris in January 2015 – shows that, in a democracy, human rights may be fragile in times of threat.

Democratic and the EU

Respect for democracy on the internet also requires governments and governmental bodies themselves to have sufficient legitimacy. Primary EU law contains a procedural principle that is designed to contribute to liberty and democracy: as part of the democratic principles, the EU institutions have to maintain an open, transparent and regular dialogue with representative associations and civil society.

In this study, the democratic legitimacy of the European Union itself as an actor will be prominently addressed. More specifically, the need for democratic legitimacy or accountability has to be reconciled with the independence of supervisory agencies under Article 16(2) TFEU and Article 8(3) Charter. Furthermore, since governments are increasingly dependent on private parties, this trend needs to be examined from the perspective of democratic legitimacy.

5. Ambitions of the EU in promoting the Rule of Law: how to ensure Effective Privacy and Data Protection on the Internet under the Rule of Law

This section discusses the ambitions of the European Union in promoting the rule of law in relation to privacy and data protection on the internet. This relation is problematic, as illustrated by the Snowden revelations, big data and other developments in the information society. It is not evident that the rule of law is always respected. Under the rule of law, there must be control of power, while people are also entitled to effective legal protection. There is a close link between the rule of law and elements of the right to data protection.

Understanding the concept of the rule of law

---

87 There is a great deal of case law on this. The well-known example, discussed in other parts of this study, is Joined Cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461.
89 Article 11(2) TEU.
90 See Chapter 4 of this study.
91 This is the subject of Chapter 7.
92 See Chapter 3.
93 All mentioned in Chapter 3 of this study.
Although there is no generally accepted definition of the rule of law (or État de droit in French, or Rechtsstaat in German and Dutch) that derives from the various national traditions,\(^{94}\) there is wide consensus that this notion plays an essential role in our societies. As the Commission states, “The rule of law is the backbone of any modern constitutional democracy”.\(^{95}\) The European Court of Human Rights has also regularly stated that a democratic society is based on or governed by the rule of law.\(^{96}\) In *Les Verts v European Parliament* (1986), the Court of Justice referred for the first time to what was then the European Economic Community as a “Community based on the rule of law”,\(^{97}\) which meant that it provides for a complete system of judicial review.

One can consider the rule of law either as a more formal or as a more substantive notion. In the more formal – narrower – sense, the notion of the rule of law entails strong public institutions that should respect procedural requirements, while a more substantive – broader – understanding also includes substantive justice.\(^{98}\) These two understandings are regularly referred to as ‘thin’ theories, emphasising the formal/procedural aspects of the rule of law, and as ‘thick’ theories that also incorporate substantive notions of justice.\(^{99}\) In the EU context, a ‘thicker’ approach is usually taken, thus reflecting a broad and substantive understanding of the rule of law,\(^{100}\) although it is also argued that Article 2 TEU reflects a ‘thin understanding’ by distinguishing the rule of law from other core values of the European Union, such as democracy and fundamental rights.\(^{101}\)

Other commentators underline two core elements, namely the establishment of order in a society through law, on the one hand, and the control of power, on the other hand. These are different aims, which are not necessarily convergent.\(^{102}\) Individuals may require the government to act in order to ensure that private actors obey the law, and more generally that the state addresses threats, whereas under the rule of law they are also protected against acts of governments themselves. If applied to privacy and data protection: governments set the rules in order to ensure that the private sector respects these rights, whereas at the same time individuals need protection against governments.

---


\(^{96}\) E.g., *Hirst v United Kingdom*, Application No 74025/01, at 58: “An effective and meaningful democracy governed by the rule of law”.


\(^{98}\) Armin von Bogdandy, Michael Ioannidis, “Systemic deficiency in the rule of law: What it is, what has been done, what can be done”, *CMLR* 51 (2014), Issue 1, pp. 59-96, at 62 (with references to a vast literature).

\(^{99}\) L. Pech, “Rule of law as a guiding principle of the European Union’s external action”, Centre for the Law of EU External Relations (CLEER), T.M.C. Asser Institute, mainly footnote 8; Brian Tamanaha, A Concise Guide to the Rule of Law, (St. John’s University School of Law, 2007).

\(^{100}\) L. Pech, “Rule of law as a guiding principle of the European Union’s external action”, Centre for the Law of EU External Relations (CLEER), T.M.C. Asser Institute, at 8. This also follows from the case law mentioned in this paragraph.

\(^{101}\) Armin von Bogdandy, Michael Ioannidis, “Systemic deficiency in the rule of law: What it is, what has been done, what can be done”, *CMLR* 51 (2014), Issue 1, pp. 59-96, at 62-63.

In addition, the separation of powers and the independence of the judiciary are considered elements of the rule of law. In Assanidze v Georgia the European Court of Human Rights set a standard precluding the legislature from interfering with the administration of justice to influence the judicial determination of a dispute, from calling a ruling into question and from preventing its execution. This case law may have relevance in relation to the independence of data protection authorities.

These different interpretations are mentioned in order to illustrate that the rule of law is a core value for the European Union, as well as for the Member States, but that there is no consensus as to what this value precisely comprises. In the context of this study, we follow what Von Bogdandy and Ioannidis see as the essence of the rule of law. According to them, the rule of law “requires as a minimum that the law actually rules”. Public authorities must act in accordance with the law and ensure that private actors observe the law.

The rule of law and its relation to fundamental rights

There is abundant literature on the rule of law and its relation to fundamental rights. This does not imply that consensus exists on the nature of this relationship. However, it is beyond doubt that the need for respect of the rule of law has implications for the protection of fundamental rights, as stated in the preamble of the Universal Declaration of Human Rights: “Whereas it is essential, if man is not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law”. The case law of the Court of Justice also underlines this relationship. The Court ruled in UPA that “The European Community is, however, a community based on the rule of law in which its institutions are subject to judicial review of the compatibility of their acts with the Treaty and with the general principles of law which include fundamental rights.”

The relationship between the rule of law and fundamental rights contains various elements. Firstly, respect for the rule of law requires, in general terms, the effectiveness of protection of fundamental rights, while, secondly, legality has to be ensured. Article 52(1) Charter reflects this, insofar as it requires restrictions on the exercising of fundamental rights to be prescribed by a law. This requirement of Article 52(1) is similar to provisions of the European Convention on Human Rights. Legality plays an important role in the case law of the European Court of Human Rights and is developed into quality standards of accessibility and foreseeability.

104 Assanidze v Georgia, Application No 71503/01, 8 April 2004, at 129-130.
105 See mainly Chapters 7 and 8 of this study.
106 Armin von Bogdandy, Michael Ioannidis, “Systemic deficiency in the rule of law: What it is, what has been done, what can be done”, CMLR 51 (2014), Issue 1, pp. 59-96, at 63.
Effective legal protection for everyone

The rule of law implies that individuals are entitled to effective judicial protection of the rights they derive from the EU legal order, as underlined in the case law of the Court of Justice. In this sense, the rule of law is also reflected in the fundamental right of Article 47 Charter (which in turn is based on Article 6 ECHR). This fundamental right to effective legal protection also includes the provision of legal aid to those who lack sufficient resources, insofar as such aid is necessary to ensure effective access to justice.

Effective legal protection should be given to everyone, including those adhering to the philosophy of terror. The Court of Justice ruled in Kadi and Al Barakaat that also persons to whom restrictive measures – such as the freezing of their financial assets – are addressed have a right to be informed of the grounds on which these measures are based, in order to be able to defend their rights in the best possible conditions.

However, this does not mean that restrictions on such people are not possible if required for reasons of national security. As Advocate General Bot articulated in ZZ, “In a democratic society, it is imperative to allow the very people who are fighting the safeguards provided by the rule of law to benefit from those same safeguards in order to ensure the absolute primacy of democratic values, but this cannot result in a kind of suicide of democracy itself.”

The rule of law has a close link with the right to data protection

Effective judicial protection under the rule of law has a close link with the right to data protection, as specified under Article 8(2) Charter and in Directive 95/46 on data protection. To illustrate this link, Article 8(2) Charter includes the right of the data subject to have access to data that have been collected concerning him or her, whereas Articles 10 and 11 of Directive 95/46 provide that information must be given to the data subject (the ‘right to information’).

111 Case C-50/00P, Unión de Pequeños Agricultores v Council of the European Union, EU:C:2002:462, at 39 and other cases cited in previous footnotes. Although it would have been logical to discuss effective judicial protection under the heading of ‘fundamental rights’, this study followed the case law in this by considering this subject under the rule of law.
113 This addition stems from the case law of the ECtHR. See: Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 47.
115 Case C-300/11, ZZ, EU:C:2013:363, Opinion AG, at 43.
117 The right of access provided in Article 8 Charter is elaborated in Article 12 of Directive 95/46.
The Court of Justice interpreted the right to effective judicial protection in ZZ, a case on secret evidence and due process rights, to include the requirement that “the parties to a case must have the right to examine all the documents or observations submitted to the court for the purpose of influencing its decision, and to comment on them”.\(^\text{118}\) Parties in a criminal case must always be informed of the essence of the grounds of a decision taken against them.\(^\text{119}\) In Kadi and Al Barakaat, as mentioned before, the Court took the same line in relation to persons to whom restrictive measures are addressed.\(^\text{120}\)

Although these rulings of the Court were based on the right to effective judicial protection, similar arguments could be based in substance on the rights of data subjects under data protection law. This explains the involvement of the European Data Protection Supervisor in the assessment of restrictive measures;\(^\text{121}\) in other words, effective redress under the rule of law relates not only to the protection of fundamental rights in general, but is also reflected in the rights of the data subject under EU data protection law.

In Schrems, the Court does make an explicit link between the rights protected under data protection law and the fundamental right to effective legal protection. It ruled that the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 Charter, is not respected if an individual cannot “pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data.”\(^\text{122}\)

Since the effective redress, or lack of it, in an internet environment is a main theme in privacy and data protection, the subject of redress under the rule of law returns in various parts of this study. A specific and recurring issue in the negotiations with the United States, for instance, is that, under the US Privacy Act, non-US residents do not have access to US courts, even where EU citizens’ personal data are transferred to the US.\(^\text{123}\) This does not comply with the rule of law, as understood in the context of EU law, as confirmed by the Court of Justice in Schrems.\(^\text{124}\)

\(^{118}\) Case C-300/11, ZZ, EU:C:2013:363, at 55, and the case law mentioned there.
\(^{119}\) For more detail, see: Nik de Boer’s case note “Secret evidence and due process rights under EU law: ZZ”, CMLR 51 (2014), Issue 4, pp. 1235-1262.
\(^{120}\) Joined Cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461, at 336-337.
\(^{122}\) Case C-362/14, Schrems, EU:C:2015:650, at 95.
\(^{123}\) Unlike the Freedom of Information Act, the US Privacy Act covers only US citizens and permanent residents. Thus, only a citizen or permanent resident can sue under the US Privacy Act; see: https://epic.org/privacy/1974act/. The problem is recognised on the US side, and the Obama administration is seeking support to change this; see: http://www.justice.gov/opa/pr/2014/June/14-ag-668.html. See also Chapter 6 of this study.
\(^{124}\) Case C-362/14, Schrems, EU:C:2015:650, at 90 and 95.
6. Ambitions of the EU in promoting Fundamental Rights: understanding the Context of Privacy and Data Protection and the Internet under EU law

This section explains a few specific elements of fundamental rights protection so as to enable an understanding of privacy and data protection on the internet in a European Union based on values. These are elements that outline some basic features of fundamental rights protection by focusing on specific dimensions of the internet. Section 7 is dedicated to a subject that gains a new dimension on the internet: fundamental rights protection in horizontal relationships vis-à-vis private parties, particularly with regard to privacy and data protection. Since the protection of fundamental rights in the Union is to a large extent the result of the case law of the Court of Justice and, indirectly, of the European Court of Human Rights, Sections 6 and 7 are closely connected to the – more elaborate – substance of Chapter 5 on the role of the Court of Justice under Article 16 TFEU.

The broad applicability of fundamental rights: application in all situations

As the strategic guidelines adopted by the European Council in June 2014 under Article 68 TFEU confirm, full respect of fundamental rights is key in EU policies. More particularly, the guidelines state that “[A]ll the dimensions of a Europe that protects its citizens and offers effective rights to people inside and outside the Union are interlinked”. The Court of Justice took the same view – although formulated in a different way – in Åkerberg Fransson by stating that “situations cannot exist which are covered […] by European Union law without those fundamental rights being applicable. The applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter.”

The scope of application ratione personae of fundamental rights protection under the Charter is also broad. Many provisions in the Charter protect “everyone”, thus confirming the universal nature of the protection of the rights included in these provisions, amongst which Articles 7 and 8 Charter. However, some rights of the Charter have a more limited personal scope in that they are restricted, for example, to EU citizens.

The Court of Justice confirmed in Kadi and Al Barakaat the applicability of the fundamental rights to all situations by ruling that “[T]he obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights”. Neither this ruling nor this statement is fully uncontroversial, both, however, reflect the current state of EU law and confirm the external effect of EU fundamental rights.

---

126 Case C-617/10, Åkerberg Fransson, EU:C:2013:105, at 21.
127 See Title V of the Charter.
129 E.g., the contributions of De Búrca and Halberstam in: Gráinne de Búrca and J.H.H. Weiler (eds), The Worlds of European Constitutionalism (Contemporary European Politics), (Cambridge University Press, 2012).
This case law is in line with Article 21 TEU, which expresses the universality and indivisibility of human rights and fundamental freedoms in relation to external action of the European Union. Under Article 3(5) TEU, European values are not confined to the territory of the Union: “In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens.” Article 21 TEU elaborates: “The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement”. Article 21(3) TEU then clarifies that these principles should not only guide the Union’s external action, but also the external aspects of all its policies. The European Council states in its famous Laeken Declaration on the future of Europe (2001) that the Union seeks to set globalisation within a moral framework.

Although fundamental rights are applicable to all situations within the scope of EU law, this broad applicability does not extend the competence of the Union. Instead, the broad applicability is a consequence of the broad objectives and activities of the Union, which are a source of interpretation for the Court of Justice.

Most fundamental rights, including the rights to privacy and data protection, are not absolute rights. Article 52(1) Charter specifies that the exercising of rights may, under certain conditions, be limited. The limitation must be provided for by law, while the essence of the rights must be respected and the limitation must be proportional. A proportionality test is at the core of the Court’s review of limitations of fundamental rights and takes various factors into account. The Explanations to the Charter specify that the wording of Article 52(1) Charter was taken from the case law of the Court of Justice. Limitations should “not constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights”.

A different test is applied in the specific situation of when two fundamental rights in the Charter need to be balanced.

Fundamental rights protection and the internet

The broad applicability of fundamental rights has specific relevance in connection with the complex and developing information society. Individuals are entitled to the protection of their fundamental rights when they are active on the internet (online), in the same way as when they are acting in any other capacity (offline). In principle, the outcome must be the same:

---

130 This is also specified in Article 21(2) TEU, which – as far as relevant here – reads: “The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to: (a) safeguard its values, fundamental interests, security, independence and integrity; (b) consolidate and support democracy, the rule of law, human rights and the principles of international law.”


132 Koen Lenaerts and Piet van Nuffel, European Union Law (third edition), (Sweet & Maxwell, 2010), at 111. On EU competence, see Chapter 4 of this study.

133 Case 270/80, Polydor, EU:C:1982:43, at 16, on “interpretation in the light of the Community's objectives and activities as defined by Articles 2 and 3 of the EEC Treaty”.

134 Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 52.

135 See Chapter 5, focusing on exceptions and derogations to the rights to privacy and data protection.

136 See also the UN Resolution affirming that the same rights that people have offline must also be protected online: UN General Assembly, Human Rights Council, “The promotion, protection, and enjoyment of human
the same level of protection must be afforded independently of the circumstances and situations requiring protection, be they online or offline. And the EU institutions and bodies – and the Members States, as far as they act within the scope of EU law – are obliged to ensure this.

In an internet environment, the protection of EU citizens extends to acts of third-country companies and authorities. Protection against actors outside the European Union is an inherent part of the protection that must be given, as provided for in the Treaties. Protection is needed in situations where EU citizens do not actively move outside the Union, or sometimes do not even engage with third-country companies, such as where citizens’ personal data are transferred to third countries, sometimes even without their knowledge, because European governments or companies use non-EU cloud providers.

There is a similar need for protection where parties in third countries (companies and/or authorities) have access to data stored in Europe. An example of the latter is the transfer of personal data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. Under the agreement between the EU and the US, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) as a designated provider provides certain financial data of residents of the EU to the US Treasury Department.

The broad applicability does not necessarily mean that individuals are entitled to protection against all risks on the internet. Effective protection against all risks – a zero-risk approach – would be difficult to achieve, as this study explains in relation to privacy and data protection. Moreover, fundamental rights coincide and sometimes collide with other fundamental rights and public interests. Trade-offs therefore have to be made, as in the case, for instance, of the trade-off between privacy and security.

7. **Fundamental Rights Protection against Private Parties acquires a new Dimension on the Internet, particularly for Privacy and Data Protection**

Privacy and data protection need to be ensured on the internet in relationships between individuals (‘data subjects’) and data controllers; in many situations, the latter are private
parties, including big internet companies, with a strong market position. Situations where individuals are engaged with other individuals or legal persons under private law are referred to as horizontal situations. The specific importance of the protection of individuals against acts of private parties on the internet justifies discussing these horizontal situations in a separate section.\footnote{See, on powers on the internet, Chapter 3.}

The applicability of the Charter in purely horizontal situations remains unclear.\footnote{The dispute is not horizontal. Mirjam de Mol, “The novel approach of the CJEU on the horizontal direct effect of the EU principle of non-discrimination: unbridled expansionism of EU law?”, Maastricht Journal of European and Comparative Law, 2011 (1-2) pp. 109-135, at 110.} The issue of whether it is applicable may arise in a civil dispute between two private parties – the data subject and the data controller – but also during an enforcement action of a supervisory authority against a private data controller. Although the latter situation may not necessarily qualify as horizontal,\footnote{As broadly interpreted in Case C-617/10, Åkerberg Fransson, EU:C:2013:105.} the underlying issue is the same: is the Charter directly binding on private parties?

At first sight, the answer to the question of whether the Charter applies in horizontal situations seems to be negative. The Charter does not protect individuals against other individuals or legal persons under private law, and nor does it bind private parties. Article 51 Charter is addressed to the EU institutions and bodies, and to the Member States when they are implementing EU law.\footnote{Case C-152/84, Marshall I, EU:C:1986:84, at 48.} This would mean that private parties, such as the big companies processing large amounts of personal data on the internet, are \textit{prima facie} excluded from the personal scope of the Charter. There is a parallel here with the denial of direct effect of EU directives expressly directed at Member States and not at individuals.\footnote{See: Paul Craig and Gráinne de Búrca, EU Law, Text, Cases and Material (Fifth Edition), (Oxford University Press, 2011) and the literature mentioned there.}

At second glance, however, the answer is not evident, despite the fact that much has been written on the horizontal direct effect of EU law,\footnote{E.g., L.F.M. Verhey, Horizontale werking van grondrechten, in het bijzonder op het recht van privacy (W.E.J. Tjeenk Willink, 1992).} as well as on the application of fundamental rights in relations between private parties (in horizontal situations),\footnote{E.g., Ward in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014), under the heading “Issues yet to be fully resolved by the Court”. See also: Mirjam de Mol, “The novel approach of the CJEU on the horizontal direct effect of the EU principle of non-discrimination: unbridled expansionism of EU law?”, Maastricht Journal of European and Comparative Law, 2011 (1-2), pp. 109-135; Allan Rosas and Lorna Armati, EU Constitutional Law, an Introduction (Hart Publishing, 2010), at 179-180.} including in connection with the Charter.\footnote{Case C-152/84, Marshall I, EU:C:1986:84, at 48.} Contrary to first impressions, therefore, the main arguments support the direct applicability of the Charter – in particular, provisions of the Charter with sufficient precision – in horizontal situations.

\textit{Four arguments supporting direct applicability in horizontal situations}
Firstly, the Charter is part of EU law and even has the same status as the Treaties. One of the basic foundations of EU law – as far back as *Van Gend & Loos*148 – is that, under certain conditions, individuals have directly enforceable rights and duties, also vis-à-vis other individuals.149 Article 51(2) Charter does not extend the field of application of EU law, although, on the other hand, the Court of Justice declared in *Åkerberg Fransson* that situations cannot exist within the scope of EU law without the fundamental rights in the Charter being applicable.150 In this hypothesis, the horizontal effect of the Charter would be the consequence of the existence of directly enforceable rights and duties within the scope of EU law.

Secondly, the issue has been brought before the Court of Justice, but the case law is not yet fully clear. In *Association de médiation sociale*,151 the Court ruled that Article 27 Charter cannot be invoked in a dispute between individuals. In its reasoning, however, the Court put great emphasis on the specific wording of this article, which is not appropriate to be directly invoked. This contrasts with the facts that gave rise to *Kücükdeveci*152 “in so far as the principle of non-discrimination on grounds of age at issue in that case, laid down in Article 21(1) Charter, is sufficient in itself to confer on individuals an individual right which they may invoke as such.” This supports the argument that certain provisions of the Charter may be applicable in horizontal situations, on the basis of a reasoning a contrario.

However, the Court has not provided full clarity in this respect since *Kücükdeveci*153 was not decided on the basis of the Charter,154 but on the basis of a provision of a directive with direct effect and with the same substance as Article 21(1) Charter on the discrimination on the basis of age. Commentators have criticised155 the Court for accepting that the Charter’s prohibition of discrimination can be invoked in relations between private parties, despite the fact that the Explanations relating to the Charter state that Article 21(1) does not impose a sweeping ban on discrimination.156 In this hypothesis, the horizontal effect would be the consequence of the case law on non-discrimination.

Thirdly, an important rationale in the development of the right to data protection in the 1970s – in addition to the right to privacy – was precisely the possible misuse of personal information in the private sector.157 Moreover, Article 8 Charter, which establishes the right

---

150 Case C-617/10, *Åkerberg Fransson*, EU:C:2013:105, at. 21.
153 In this sense, see: Cian C. Murphy, “Using the EU Charter of Fundamental Rights Against Private Parties after Association de Médiation Sociale”, *European Human Rights Law Review*, (2014), at 170.
154 Although the ruling, dating from 19 January 2010 (i.e. just after the entry into force of the Lisbon Treaty), mentions the Charter.
to data protection, has Directive 95/46 as one of its main sources, the provision originates from a directive based on an internal market legal basis, currently Article 114 TFEU.

Even where the Charter or provisions in the Charter do not apply directly in horizontal situations, they may apply indirectly because courts interpret instruments of EU law in the light of the Charter. Examples of this can be found in the case law of the Court of Justice that take account of the significance of a fundamental right in the Charter when interpreting an EU directive. In this hypothesis, the horizontal effect – under the doctrine of sympathetic interpretation – is based on acts of the legislator.

Fourthly, the indirect application may also be the result of a positive duty of governments to protect. Where fundamental rights serve as protection against breaches by acts of government itself, the obligation of the government can be described as negative: refrain from action. The government, however, also has a positive duty, and that is to ensure that fundamental rights are effectively protected in horizontal situations.

This is all the more important in the context of the internet, where essential risks of breaches of fundamental rights are caused by actions of private companies. Dominant economic players on the internet have a strong position, and this hampers the achieving of the objective that the same protection should be given online as offline. In this hypothesis, the horizontal effect would find its origin in the principle of effectiveness. A fundamental right would be ineffective if it protected only against governments.

All in all, there are good arguments supporting the applicability of certain fundamental rights of the Charter in horizontal relations, in particular on the internet. These arguments are even more convincing for privacy and data protection since one of the reasons why the concept of data protection emerged was the possibility of personal information being misused by the private sector. Outside the internet context, the European Court of Human Rights has accepted horizontal application of the right to privacy under Article 8 ECHR.

---

158 Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 8. This is elaborated in Section 10.
159 E.g., Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777, at 39-40: “Article 7(f) of Directive 95/46 […] necessitates a balancing of the opposing rights and interests […] [T]he person or the institution which carries out the balancing must take account of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union”.
161 This positive duty or, in German, Schutzpflicht is discussed in relation to privacy in Section 9.
162 As explained in Chapter 3.
164 The ECtHR ruled that “… in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves”. See, e.g., Von Hannover v Germany, 2004, Application No 59320/00, at 57.
8. The Right to Privacy, a Broad and Dynamic Concept on the Internet extending to the Public Sphere

Historical development of privacy, starting with Warren & Brandeis

The right to privacy is a concept with a history going back further than the European Convention on Human Rights. In 1890 Warren & Brandeis wrote a paper, published in the Harvard Law Review,\(^\text{165}\) which is seen as the origin of this right.\(^\text{166}\) This paper is still worth reading because it describes the right to privacy as a “principle which protects personal writings and any other productions of the intellect or of the emotions”. The authors also mention “the right to be let alone”.\(^\text{167}\) This idea of a right to be let alone is retained by Westin, who wrote an authoritative study on privacy at the dawn of the computer age (1967). He describes privacy in relation to social participation as the voluntary and temporary withdrawal of a person from general society, adding that the individual’s desire for privacy is never absolute since participation in society is an equally powerful desire.

The paper of Warren & Brandeis also distinguishes the right to privacy from other rights, such as intellectual property rights and the right of freedom of expression. The right to privacy received international recognition immediately after the Second World War in Article 12 of the Universal Declaration of Human Rights and later, in 1966, in Article 17 of the International Covenant of Civil and Political Rights.

In Europe, the right to privacy or a private life is included in Article 8 ECHR, which protects private and family life, home and correspondence. The scope of this definition is wider than privacy or private life as Article 8 ECHR and the corresponding Article 7 Charter\(^\text{168}\) also protect values not connected to privacy, such as the right to respect for family life that relates to other areas of EU law, such as gender equality, children’s rights and free movement, immigration and asylum.\(^\text{169}\)

In accordance with their text, these articles protect privacy and three other fundamental rights.\(^\text{170}\) However, apart from what was mentioned in relation to family life, the distinction between privacy and these other rights is not always fully clear. This is exemplified by the right to respect of correspondence (in Article 7 Charter: communications), which is a specific


\(^{166}\) Although this can be disputed. Warren & Brandeis themselves mention an earlier French law, the Loi relative à la presse (11 Mai 1868): “11. Toute publication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'une amende de cinq cent francs. La poursuite ne pourra être exercée que sur la plainte de la partie intéressée.” Rivière, Codes Français et Lois Usuelles. App. Code Pen., at 20.


\(^{168}\) As explained by the Explanations relating to the Charter of Fundamental Rights (on Article 7), a slight change was made to Article 8 ECHR: as a result of developments in technology, the word ‘correspondence’ has been replaced in Article 7 Charter by ‘communications’.


\(^{170}\) Further explained by Paul De Hert, Art. 8 E.V.R.M. en het Belgisch Recht, Bescherming van privacy, woonst, gezin en communicatie (Mys en Breesch, 1998).
aspect of privacy, as demonstrated by the case law of the European Court of Human Rights on secret surveillance. This case law takes the respect of privacy and correspondence together.\textsuperscript{171}

A specific element of the concept of privacy – of relevance for the purpose of this study – is the concept of informational privacy, as originally developed in the work of Westin.\textsuperscript{172} On the internet, the right to privacy, by definition, concerns information, and does not touch upon more spatial concepts of privacy, such as the protection of a person’s home. In any event, technological developments meant that informational privacy became a central element of privacy protection.\textsuperscript{173} This study, with its focus on the internet, obviously deals mainly with this informational privacy. Finally, informational privacy should not be confused with ‘data privacy’, a term used outside the EU context for a concept that also includes data protection.\textsuperscript{174}

**Human dignity and personal autonomy as underlying values and the broad scope of privacy**

The ECHR and the Charter do not refer to any underlying values in relation to privacy.\textsuperscript{175} One can argue that the right to privacy, as described by Warren & Brandeis, reflects a value in itself. This right reflects individuality or personal freedom\textsuperscript{176} and may even be opposed to societal needs.\textsuperscript{177} The arguments of Greenwald, referred to in Section 3 of this chapter, illustrate that privacy itself reflects a value, namely the value of doing things in private. In addition, one can argue – also illustrated by what Greenwald said – that the right to privacy is a representation of other core ethical values in society,\textsuperscript{178} particularly human dignity and autonomy.

Privacy is explained as a representation of human dignity. Privacy is not unique in this respect, as confirmed by the Explanations to the Charter with reference to the Universal Declaration of Human Rights: human dignity constitutes the real basis of fundamental

\textsuperscript{171} See, e.g., *Klass and Others v Germany*, 1978, Application No. 5029/71, at 41.
\textsuperscript{174} As explained later, the distinction between privacy and data protection is a typically European distinction. See, e.g.: Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013), at 21, where he deals with data privacy law in a global context, encompassing privacy and data protection.
\textsuperscript{176} G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2014, referring to a source mentioning the fortress of personal freedom.
\textsuperscript{177} Lee A. Bygrave, “Privacy and Data Protection in an International Perspective”, Stockholm Institute for Scandinavian Law & Lee A. Bygrave 2010, at 171.
Where, however, dignity is understood as the freedom to shape one’s life, there is a specific association with privacy. Privacy is also described as a right to personal autonomy, which implies that an individual must be in control of his or her life. Fabre argues that autonomy reflects a value underlying all fundamental rights. Autonomy in connection with the right to privacy is more limited and relates to an autonomous personal sphere; this does not mean a limitation to intimacy, but, as explained below, also extends to wider social relations. As González Fuster explains, privacy is sometimes, but not always, construed as being the opposite of what is public. In this widely understood autonomous personal sphere individuals must have some control over how information about them is used.

As to the scope of privacy: according to the ECtHR the concept of ‘private life’ is a broad term, which is not susceptible to exhaustive definition. Privacy is a notoriously difficult legal concept. In the case law, the notion of privacy or private life has been given a broad scope and also extends to professional and business activities. More generally, privacy includes the right to establish and develop relationships with other human beings and the outside world. Equally, the ECtHR ruled in Rotaru v Romania that public information, too, can fall within the scope of private life, but only if it is systematically collected and stored in files held by the authorities. Finally, all modern means of communications are brought under the scope of privacy of Article 8 ECHR.

As De Hert and Gutwirth confirm, a broad and dynamic interpretation was assigned to the right to privacy under Article 8 ECHR. This approach also determines the interpretation of the corresponding right of Article 7 Charter since the meaning and scope of this corresponding right must be the same and must not

---

179 Explanations relating to the Charter of Fundamental Rights, on Article 1.
180 Cathérine Dupré on Article 1, in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014), e.g., at 01.06.
181 P. Oliver, “The protection of privacy in the economic sphere before the European Court of Justice”, CMLR 46 (2009), Issue No (Oct), at 1443. In the same sense, P. Bernal, Internet Privacy Rights, Rights to Protect Autonomy (Cambridge University Press, 2014), at 2. He defends the belief that privacy is mainly important as a crucial protector of autonomy.
182 In this sense, it is close to the right to data protection, as developed below.
185 As will be explained in relation to data protection, this does not necessarily mean full control.
187 E.g., Pretty v UK, Application No 2346/02, at 61.
188 This was said about the right to human dignity in Article 1 Charter by Cathérine Dupré in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014) at, e.g., 01.26.
190 E.g., Pretty v UK, Application No 2346/02, at 61.
191 Rotaru v Romania, Application No 28341/95, at 43.
prevent more extensive protection under EU law. However, this broad and dynamic interpretation does not necessarily mean that the ECtHR includes all use of personal information within the scope of privacy. It is this limitation to the scope of privacy that is challenged in Sections 13 and 14 below.

The internet also presents challenges to another limitation to the scope of the right to privacy, at least insofar as privacy is limited to what is not public. More specifically, the difference between shared, exposed and common activities, which are open to others, and activities belonging to the closed space or realm — or, more generally, the distinctions between the public sphere and the private sphere — are becoming blurred, with Web 2.0 and exposure on social media being obvious examples. These developments are not strictly linked to the internet, as the Court’s ruling in *Ryneš* illustrates. This ruling concerns the use of a CCTV camera by a private person in order to protect his private home that involved capturing images from a public space near his home.

This all makes privacy an even more difficult legal concept than before, because it also further widens the area where claims are made based on the right to privacy beyond the already broad scope of privacy recognised in the case law of the ECtHR.

9. **Understanding the Nature of the Right to Privacy through four types of Qualified Interests: Information use by Governments, Health, Vulnerable Groups and Reputation**

The right to privacy is a ‘first-generation’ right that imposes a negative duty to refrain from interfering with the exercise of the right by the individual. Privacy, as a legal notion, protects the private sphere of the citizen, primarily against intervention by the state. The fact that privacy is primarily as a duty for governments to abstain explains why, at an EU level, no general legal instrument comparable to the general instruments for data protection, such as Directive 95/46, has been adopted for the protection of the right to privacy. However, there is more to it than that. The state also has a positive duty to ensure that the right to privacy is respected in horizontal situations between private actors. This has led to

---

193 As stated in Article 52(3) Charter.
196 See also Chapter 3 of this study.
197 *Case C-212/13, Ryneš, EU:C:2014:2428.*
200 This is more complicated, but a general theory of privacy is not necessary for this study. See also: G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2014, Chapter 2 and the literature mentioned there.
201 According to the case law of the ECtHR: “... in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the
legislative provisions in a wide area of government intervention, thus specifying privacy protection in various sectors of society. Moreover, as we have seen in Digital Rights Ireland and Seitlinger, where the legislature imposes interference on the right to privacy, it should also ensure that appropriate safeguards are foreseen.

As explained above, privacy must be seen as a normative value representing the human dignity and autonomy of an individual. It is a broad concept that – to a certain extent – encompasses the public sphere. Privacy must be interpreted in a broad and dynamic way. This is further illustrated by the Court of Justice’s case law, which emphasises that non-sensitive information may also amount to interference with the right to privacy and, too, that adverse consequences are not required for such interference.

In Digital Rights Ireland and Seitlinger, the Court of Justice referred to the essence of the right to privacy in relation to personal information. The Court considered that the essence of the right to privacy – a notion defined under Article 52(1) Charter in respect of all fundamental rights – was not affected by Directive 2006/24 on data retention since this directive “does not permit the acquisition of knowledge of the content” of communications. Schrems, by contrast, concerned access to the content, i.e., the inverse situation. According to the Court, generalised access to the content of electronic communications compromises the essence of the right to privacy.

One can argue whether the Court’s specific understanding of this concept of the essence of privacy makes sense in a developing information society, where traffic and location data reveal a great deal of the privacy of individuals. In any event, the Court determined that there is an area where there can be serious interference with the right to privacy, but that is outside its essence, while there is also an area where such interference compromises the essence.

Four types of qualified interests: information use by governments, health, vulnerable groups and reputation
In order to provide a better understanding of informational privacy we will explore various types of interference. In case law there are various qualified interests that may create an interference with privacy. This study considers four types of qualified: storing, monitoring and interception of information by governments; health-related information; the protection of vulnerable groups such as children, and the reputation of people in relation to publications.

Firstly, governments’ access to and use of information for policing or wider law enforcement purposes. The storing, monitoring and interception of information by governments obviously have implications for privacy. In *Malone v UK*, the European Court of Human Rights held that a telephone operator may obtain records of the ‘metering’ of its clients, but that releasing that information to the police interferes with privacy. In *Leander v Sweden*, the ECtHR ruled that the storing and release of information from a secret police file amounted to interference with privacy. More recently, the ECtHR decided in *S. and Marper v UK* that the retention for police purposes of “the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences” constituted a violation of Article 8 ECHR.

The Court of Justice stated in *Digital Rights Ireland and Seitlinger*, with reference to the case law of the ECtHR, that the access by law enforcement authorities to communications data retained by private companies under Directive 2006/24 constituted a “further interference with the right to privacy”. Likewise, the law must effectively protect individuals’ personal data against the risk of abuse and against any unlawful access and use of that data, based on the assumption that there is a significant risk of these effects occurring.

Secondly, the processing of health-related information may have a serious impact on the right to privacy. In *Z v Finland*, in which the applicant was HIV-infected, the ECtHR underlined that “respecting the confidentiality of health data is a vital principle in the legal systems [...], not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.” This need for confidentiality is even stronger in the case of a transmissible disease such as HIV.

Thirdly, special protection of privacy is given to vulnerable groups such as children. This was a constitutive element in establishing the violation of Article 8 ECHR in *K.U. v Finland*, where the applicant was the subject of an advertisement of a sexual nature on an internet

---

210 The listing in this study is meant to be illustrative, not exhaustive. A similar listing is given by Christopher Docksey, “Articles 7 and 8 of the EU Charter: two distinct fundamental rights”, in: Alain Grosjean (ed.), *Enjeux européens et mondiaux de la protection des données personnelles* (Éd. Larcière, 2015), at 4a.
211 *Malone v UK*, 1984, Application No 8691/79, at 84. Metering is the use of a device that registers the numbers dialled on a particular telephone and the time and duration of each call.
214 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*, as will be discussed in Chapter 5.
215 Para. 35 of the ruling.
216 Paras 54-55 of the ruling, with reference to case law of the ECtHR.
dating site when he was only 12 years old.\textsuperscript{218} This special protection also played a role in \textit{S. and Marper v UK} in relation to the retention of biometric data, which was considered especially harmful in the case of minors.\textsuperscript{219}

Fourthly, the reputation of individuals is an issue that affects human dignity and relates closely to the right to privacy. Reputations may be harmed by a journalistic publication or by disclosure of information to the public in any other way. Reputational issues give a good insight into the protection of privacy on the internet and play a role in the balancing between privacy (and data protection), on the one hand, and freedom of expression and public access to documents, on the other hand.\textsuperscript{220}

The most famous ECtHR cases are the two \textit{Von Hannover v Germany},\textsuperscript{221} in which Princess Caroline of Monaco was the main applicant. In the second case she was joined by her husband. As the Court considered, reputation takes on particular importance in the context of Article 8 ECHR\textsuperscript{222}, also where famous persons are concerned.

In \textit{Google Spain and Google Inc.},\textsuperscript{223} a case that is relevant to this study for a number of reasons, the right to privacy under Article 7 Charter plays an essential role in relation to reputation.\textsuperscript{224} The ruling of the Court of Justice in this case was the result of a complaint by a Spanish resident, Mr Costeja González, that relatively old pages from a Spanish newspaper came up when his name was entered in Google Search. These pages mentioned his name in relation to the recovery of social security debts. Mr Costeja González claimed that the issue had been resolved for a number of years and that the data were now entirely irrelevant. These data were neither illegal nor inaccurate, but, as Peers underlines,\textsuperscript{225} simply embarrassing.

\textit{Summing up: all use of personal information falls within the scope of the right to privacy under Article 7 Charter}

As explained above, the notion of privacy is a normative value. Interference with the right to privacy is assessed in a contextual manner.\textsuperscript{226} The four types of qualified interests illustrate how the use of personal information may constitute an interference with the right to privacy and how this interference is assessed. However, this does not answer the fundamental question of whether all use of personal information— or, in the terminology of data protection law, all processing of personal data— falls within the scope of the right to privacy and creates

\begin{itemize}
\item \textsuperscript{218} K.U. v Finland, 2008, Application No 2872/02, at 40-41.
\item \textsuperscript{219} \textit{S. and Marper v UK}, Applications Nos 30562/04 and 30566/04, 4 December 2008, at 124.
\item \textsuperscript{220} See also Chapter 5, Section 14 of this study.
\item \textsuperscript{221} \textit{Von Hannover v Germany}, 2004, Application No 59320/00 and \textit{Von Hannover v Germany (No 2)}, 2012, Applications Nos 40660/08 and 60641/08.
\item \textsuperscript{222} Para. 59 of the first \textit{Von Hannover} case.
\item \textsuperscript{223} Case C-131/12, \textit{Google Spain and Google Inc.}, EU:C:2014:317.
\item \textsuperscript{226} Orla Lynskey, “Deconstructing Data Protection: The ‘added-value’ of a right to data protection in the EU legal order”, International and Comparative Law Quarterly, Volume 63, Issue 03, July 2014, p 583.
\end{itemize}
interference with this right? This question can also be formulated differently: are qualified interests a condition for bringing the use of personal information within the scope of the right to privacy, or are they merely relevant for assessing an interference with this right?

In Österreichischer Rundfunk and others, a case adjudicated before the entry into force of the Lisbon Treaty, the Court of Justice distinguished between data processing within the scope of the right to privacy under Article 8 ECHR and processing outside this scope, with reference to the case law of the European Court of Human Rights. More generally, privacy is said to encompass data that are essentially private, and other data only if additional conditions relating to the processing apply. According to De Hert and Gutwirth in a 2009 paper, hence also before the entry into force of the Lisbon Treaty, this justifies the claim that “the old distinction between data that merits protection and data that does not still works”.

The question to be answered in this study is whether this conclusion still holds true, or whether the relevant issue is that the qualified interests merely determine the assessment of a breach of the right to privacy. For two reasons, this study takes the latter point of view. First, as explained below, since the entry into force of the Lisbon Treaty, the Court of Justice no longer makes a systematic distinction between the right to privacy and the right to data protection (data protection encompasses all use of personal information). Second, as a result of the features of the internet and developments of communications on the internet – with big data and mass surveillance as obvious examples – all processing of personal data has a potentially adverse effect on the right to privacy under Article 7 Charter, if only because one cannot know in advance the purposes for which personal information that is available in electronic databases will subsequently be used.

### 10. Historical Development of the Right to Data Protection, starting as a Response to Technological Developments

The right to data protection, included in Article 16 TFEU and in Article 8 Charter, has its origin in the 1970s and was a response to technological developments. It has also been recognised in primary EU law since the Treaty of Amsterdam (1997, entry into force 1999). Data protection is a right that not only protects against the government, but also requires active legislative intervention, as evidenced by Article 16(2) TFEU. Additionally and pursuant to Article 16(2) TFEU and Article 8(3) Charter, data protection requires control by an independent data protection authority.

There is a parallel between the origin of the right to privacy and the origin of the right to data protection. At the end of the 19th century, Warren & Brandeis found that, in the light of political, social and economic changes, the existing legal notions did not sufficiently protect

---

227 Case C-465/00, Österreichischer Rundfunk and others, EU:C:2003:294, at 73-74.
230 See also Chapter 3 of this study.
individuals. In 1981, the Council of Europe adopted Convention 108 on data protection — after long preparations — since it considered that, in view of new technologies, the national legislations at the time provided insufficient protection of individual privacy.

There is also, however, an important difference between the origins of these two rights, a difference that still plays a role in today’s debate on privacy and data protection. Whereas the right to privacy originates from the needs of individuals to be left alone, the right to data protection stems from an era in which individuals were losing control over the use of information about them, also because of the great asymmetry in knowledge and power between various players. This new reality was initially connected to the right to privacy, widening its rationale with more emphasis on informational privacy. This is still the situation in the United States, whereas in Europe the new reality has led to the development of the right to data protection.

The Council of Europe’s role in developing instruments on data protection

The Council of Europe’s Convention 108 of 1981 was the first binding international instrument on data protection. This Convention was adopted shortly after the non-binding OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and illustrates the different approach followed in Europe compared to the United States. The OECD Guidelines, to which both the US and EU Member States adhere, underline privacy and the free flow of information, whereas Council of Europe Convention 108 has data protection as its sole purpose. Data protection is defined as the right to secure for every individual “respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him”.

Council of Europe Convention 108 lists the basic principles of data protection, including the quality of data and the special protection for sensitive data. These principles were later introduced and specified in EU law. One element plays a specific role in the sequel of this section. Whereas, normally, personal data may be obtained and processed fairly and

---

231 Based on resolutions of the Committee of Ministers of the Council of Europe, from 1973 and 1974.
235 The guidelines were amended on 11 July 2013 by C(2013)79, published on the OECD website.
237 Article 1 of the Convention.
238 See also Convention 108; G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2014, at 4.2.
lawfully, the Convention contains a prohibition on the processing of sensitive data, subject to certain exceptions.

The EU: growing emphasis on respecting constitutional values in addition to the objective of market integration

In the context of the European Union, the right to data protection was first introduced in secondary law in 1995, in Directive 95/46. The recitals of this directive provide a good insight into its rationale. The processing of personal data had become more important in the various spheres of economic and social activity, and the progress made in information technology made the processing and exchange of such data considerably easier. The recitals also note a difference in levels of protection due to the existence of a wide variety of national laws, regulations and administrative provisions. Apparently, Convention 108 failed to ensure sufficient consistency.

Directive 95/46 on data protection, adopted under the internal market legal basis of the EU Treaties (now: Article 114 TFEU), harmonised the level of protection and aimed to ensure that this level was high. It thus had a double objective in that it promoted an internal market of personal data through the free flow of information on the one hand and protected the individual on the other hand. Interestingly, this directive, with its double objective, became one of the main sources of the fundamental right to data protection included in both TFEU and Charter. This double objective was confirmed by the Court in *Commission v Germany* and should be understood to mean that data protection requires a balance between the protection of the right to private life and the free movement of personal data.

The Treaty of Amsterdam first introduced data protection into EU primary law in Article 286 of the EC Treaty, a provision aimed at ensuring data protection within the institutions and bodies of the European Union itself and that led to the setting up of the European Data Protection Supervisor. The entry into force of the Lisbon Treaty (2009) marked a further step in EU data protection law by its inclusion of the right to protection of personal data in Article 16(1) TFEU and in Article 8 Charter. This has a consequence for the scope of the right to data protection as, within the scope of EU law, data protection now has to be ensured. This scope now includes the former third and second pillars of the EU Treaty, which are outside the scope of both Directive 95/46 and Article 286 of the EC Treaty.

---

239 Article 5 of the Convention.
240 Article 6 of the Convention on “Special categories of data”.
242 Recital 7.
243 Equally, recital 7.
245 In relation to this particular aspect, it resembles the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
246 Explanations relating to the Charter of Fundamental Rights, Explanation on Article 8.
248 Police and judicial cooperation in criminal matters, respectively the common foreign and security policy.
Article 16(1) TFEU and Article 8(1) Charter determine the scope of data protection at the level of the Treaties. The notion of personal data is broadly understood to mean “any information relating to an identified or identifiable natural person”. The scope *ratione personae* is also broad as the directive applies to wide categories of addressees of the data protection obligations (the ‘controllers’), as confirmed by the Court of Justice in *Google Spain and Google Inc.* The Court ruled that internet search engines may qualify as controllers. By doing so, it sought to ensure “the effective and complete protection of the fundamental rights and freedoms of natural persons”, in practice meaning all individuals within the scope of EU law, irrespective of their nationality or permanent residence.

The inclusion of data protection in Article 16(1) TFEU and Article 8 Charter suggests that the centre of gravity of the right has changed to give more importance to the objective of protection and less to the free movement of data. In *Deutsche Telekom*, in 2011, the Court ruled that Directive 95/46 on data protection is designed to ensure the observance of the right to data protection. In its recent case law, the Court has also interpreted Directive 95/46 more or less systematically in the light of the fundamental rights. Hence, the change of the legal context has given a more authoritative foundation to data protection as a fundamental right, rather than as an off-shoot of the internal market. There is a parallel in this respect with the developments in the field of non-discrimination which developed from a condition for the functioning of the internal market into a constitutional norm. This also reflects the developing role of the European Union itself, with a growing emphasis on the respect for constitutional values in addition to market integration.

A separate development in the area of freedom, security and justice, leading to a patchwork

The instruments in the area of freedom, security and justice have developed along different lines. Over the past decades, objectives of security led to the adoption – inside and outside the framework of the EU – of a number of legal instruments facilitating the use of

---

249 See also: Herke Kranenborg, in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014), at II. See also Chapter 6, Section 5.
252 See, e.g., Chapter 4, Section 9 of this study, which will also address the connection with EU citizenship.
253 Case C-543/09, *Deutsche Telekom*, EU:C:2011:279, at 50.
255 See Section 13 below.
256 As explained by Bell in: Paul Craig and Gráinne de Búrca (eds), The evolution of EU Law (Second Edition), (Oxford University Press, 2011), at 611-640.
information, including personal data, and requiring the collection and storage of and access to huge volumes of personal data for police and judicial cooperation in criminal matters and for the purposes of border checks, asylum and immigration. Although the policies in these latter fields are not primarily motivated by the objective of security, in reality external border management is closely linked to security. Some of these instruments included the setting up of European agencies and information systems. These instruments are now part of the EU legal framework, as are the European actors they established.

These instruments apply to national authorities and also to the actors at the EU level, currently Europol, Eurojust, the second-generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac. The instruments firstly reflect the increased need for the use of information for the purposes of safety and security, and secondly the expanded possibilities of use. In the context of police and judicial cooperation, the police has a greater need for use of electronic information because evidence is less likely to be found in physical documents than in abstract places ‘in the cloud’, and also because of the growing expectations of society, in particular since 9/11.

---

258 For the objectives of EU policies in these areas, see Articles 77(1), 78(1) and 79(1) TFEU. The objective most closely linked to security is the effort to combat illegal immigration and human trafficking.

259 E.g., Communication from the Commission to the European Parliament and the Council, Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, which closely links external border management to the prevention and combating of crime. This link does not mean that police authorities always have access to data collected for immigration or asylum purposes. This access is a recurring issue in relation to large-scale information systems on border management. See, Opinion of 18 July 2013 of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), at III.2.


264 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180/1.


266 The policies on border checks, asylum and immigration (Title V, Chapter 2 TFEU) are not mentioned here since, strictly speaking, those policies do not fall within the remit of security; in other words, this is not the main objective of these policies.

As a result of developing technologies, there are now, for instance, more possibilities for using biometric data on a large scale.268

Many of these instruments have a specific data protection regime, which was complemented only more recently by general EU rules on data protection, in Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.269 This general regime applies only where personal data are exchanged between authorities of more than one Member State, not when there is no cross-border element. Where the Council Framework Decision is not applicable,270 the general regime of Council of Europe Convention 108 applies. For border checks, asylum and immigration, the specific rules are complemented by the general regime of the Directive 95/46 on data protection. Declaration (21) on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation annexed to the Lisbon Treaty confirms the special nature of this area. The said Declaration (21) was used as justification for proposing a directive with specific rules on the law enforcement sector,271 and thus excluding this sector from the scope of the proposed General Data Protection Regulation.272

In short, EU law encompasses a developed data protection regime that provides for the balancing the value of a high level of security with the rights to privacy and data protection. However, this regime is not comprehensive. The term patchwork is quite regularly used to describe it.273 Despite this non-comprehensive nature, the legislative developments in the area of freedom, security and justice confirm the growing importance of data protection, independently of the internal market.

11. The Right to Data Protection: a Claim based on Fairness providing Safeguards where Personal Data are processed

The inclusion of data protection in the Charter as a right separate from the right to privacy is related to the right to informational self-determination, as developed by the German

---

268 E.g., the ambition to fully use new technology and to create access rights to automated DNA analysis files and automated dactyloscopic identification (fingerprints) systems is an important rationale behind Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/1 (‘Prüm Decision’), recitals 7 and 10.
269 OJ L 350/60.
270 Because of the limitations in the scope of application in its Article 1(2) or because of the precedence given in Article 28 to previously adopted acts of the Union.
271 Recital (10) of the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.
272 Article 2(2)(e) of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.
constitutional court [Bundesverfassungsgericht] in 1983.\textsuperscript{274} Earlier drafts of what is now Article 8 Charter were even similar to informational self-determination, and mentioned that an individual has a right to determine the disclosure and use of his or her personal data.\textsuperscript{275} However, the wording in the final text of the Charter is different.

Whereas it seems evident that the inclusion in the Charter of a separate right to data protection was inspired by developments in Germany, controversy exists as to whether the final text must be interpreted in the light of the right to informational self-determination.\textsuperscript{276} This controversy is relevant because it provides insight into the rationale of the right to data protection: does it serve to give an individual control over his or her personal information, or is it a claim based on fairness, providing safeguards when personal data are processed?\textsuperscript{277}

\textit{Does the right to data protection serve to give an individual control over personal information?}

In the first hypothesis, based on the right to informational self-determination, the individual (‘data subject’) has a right to prevent the processing of personal data. The individual has a right that is comparable to ownership of his personal data,\textsuperscript{278} and processing of such data always requires the consent of the individual.\textsuperscript{279} In this hypothesis, data protection is essentially a right aimed at reducing information and power asymmetries in an information society\textsuperscript{280} by giving the data subject control over the processing. An argument in support of this hypothesis is that Article 8(1) Charter is formulated as a positive right to data protection. If this right created only a claim of fairness, this would not do justice to the unconditional

\textsuperscript{275} See also: G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2014, at 6.4.1.
\textsuperscript{280} Orla Lynskey, “Deconstructing Data Protection: The ‘added-value’ of a right to data protection in the EU legal order”, International and Comparative Law Quarterly, Volume 63, Issue 03, July 2014, notably at 592-597 and literature mentioned there.
Is the right to data protection a claim based on fairness, providing safeguards where personal data are processed?

In the second hypothesis, a right to prevent processing does not exist. In the words of Hustinx, data protection “was not designed to prevent the processing of such information or to limit the use of information technology per se”. In this hypothesis, Article 8(2) contains the substantive elements of the right to data protection itself. The key criteria can be found in the first sentence of Article 8(2) Charter, which requires personal data to be “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”. Fairness and purpose limitation are the determining factors, and consent of the individual is only one of a number of legitimate bases for processing.

The second hypothesis is further supported by Article 7(f) of Directive 95/46 on data protection, which, subject to a balancing test, allows processing “necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed”. As explained above, Directive 95/46 was at the basis of Article 8 Charter. In ASNEF and FECEMD, the Court of Justice accepted that Article 7(f) of Directive 95/46 necessitated a balancing of the opposing rights and interests, provided that the significance of Articles 7 and 8 Charter was taken into account. In Google Spain and Google Inc., the Court also emphasised that Article 7(f) necessitates a balancing of the opposing rights and interests concerned. Article 7(f) is the basis for the processing of personal data by a search engine.

---

281 This view can be based on a reading where Article 8(2) and Article 8(3) Charter are seen as limitations of the right; see: Gloria Gonzalez Fuster and Serge Gutwirth, “Opening up personal data protection: a conceptual controversy”, Computer Law & Security Review (CLSR) 29 (2013), pp. 531-539, at 2.

282 The system with a prohibition with wide exceptions is retained in Article 9 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.


In our view, the second hypothesis prevails. This is the result of the way the Court of Justice deals with data protection, which emphasises the balancing of various interests. The balancing of interests is an elaboration of the notion of fairness and would not fit within a hypothesis where an individual is in control. We explain this view as follows. Suppose the first hypothesis were to be followed and there was a positive right to data protection under Article 16(1) TFEU and Article 8(1) Charter, based on control by the individual and with his consent as the rule. This would, in principle, mean that consent would be necessary under all circumstances and that processing on any other grounds would be impossible. Processing on a ground other than consent would be considered an exception to the right to data protection and would be subject to the strict proportionality test under Article 52(1) Charter. It is difficult to imagine how a balancing of various interests, as foreseen in Article 7(f) of Directive 95/46, could comply with this strict proportionality test for exceptions to fundamental rights.

In view of internet developments, the second hypothesis is also the realistic hypothesis, with big data being the clearest example. The issue at stake in *Google Spain and Google Inc.* provides a perfect illustration of this. Processing of personal data without consent of the data subject is a core activity of search engines. If the data subject had control over data processing, this would mean that search engines would not be able to process personal data, unless the data subject had given his consent or unless a specific legal basis were to be given for the search engines’ processing activities in accordance with Article 52(1) Charter.

The right to data protection provides for a system of checks and balances based on fairness

In *Digital Rights Ireland and Settlinger*, the Court of Justice placed emphasis on a concept of data protection, which was not mentioned yet: it closely linked data protection and data security. Data security was even referred to as an element of the essence of the fundamental right to data protection that, pursuant to Article 52(1) Charter, should always be respected.

The Court of Justice considers that Directive 2006/24 on data retention does not adversely affect the essence of the right to data protection because the directive requires certain principles of data protection and data security to be respected. Respect for these principles must entail the adoption of appropriate technical and organisational measures to avoid

---

289 Deborah Hurley explains that privacy supports autonomy, self-determination and dignity, in: Marc Rotenberg, Julia Horwitz, Jeramie Scott (eds), *Privacy in the Modern Age, The Search for Solutions* (The New Press, 2015), at 70. The position taken in this study means that autonomy and dignity, but not self-determination, are the underlying values of data protection.

290 As explained in Section 6.


292 In a paper of 2013 Gellert and Gutwirth dismissed the assumption that there is an ‘essence’ of the right to data protection (in the same way as they dismissed the essence of privacy, see footnote 283 above). This dismissal illustrates the complicated nature of the right to data protection. In view, however, of the recent case law, the statement as such is no longer valid. See: Raphael Gellert and Serge Gutwirth, “The legal construction of privacy and data protection”, *Computer Law & Security Review (CLSR)* 29 (2013), pp. 522-530.

accidental or unlawful destruction, accidental loss or alteration of the data.\textsuperscript{294} Although this explanation of the essence may not be fully clear,\textsuperscript{295} it does confirm the view that the right to data protection does not prevent data processing, but instead provides for a system of checks and balances based on fairness. The appropriate technical and organisational measures mentioned by the Court are an example of checks and balances.

However, the emphasis on fairness must not result in weak protection of a fundamental right under primary EU law.\textsuperscript{296} Taking fairness as a constitutive element of data protection does not imply that the scope of protection should be limited to situations where there is evidence of harm or risks for the data subject. It has nothing to do with the debate surrounding a risk-based approach or the accountability of data controllers and processors.\textsuperscript{297} Similarly, it also does not relate to discussions on the meaning of the consent of data subjects, in particular in the online environment. Consent as an indication of the wishes of the data subject can either be understood as ‘opt-in’ or ‘opt-out’. The first interpretation gives the individual a claim that data can only be processed if the individual has given permission (opt-in), while the latter interpretation means that the data subject must be able to object to processing (opt-out).\textsuperscript{298}

12. Data Protection as ‘Rules of the Game’ or ‘a System of Checks and Balances’

Authors argue that the right to data protection is of a different nature than the right to privacy (or other first-generation fundamental rights) since its main objective is not to protect against interference by government, but to ensure that when personal data are processed, certain legal conditions are observed.\textsuperscript{299} In other words, the right does not entail that the government (or any other party) refrains from interfering with the right by abstaining from processing.

Diverging views on the legitimacy of processing personal data

As Docksey explains,\textsuperscript{300} the processing of personal data is a condition for the application of Article 8 Charter, not an interference with it. He defines Article 8 Charter as rules of the

\textsuperscript{294} Joined Cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), at 40.
\textsuperscript{295} It is uncertain, for instance, whether the element the CJEU mentions is the only constitutive element of the essence; see: Gloria González Fuster, “Curtailing a right in flux: restrictions of the right to personal data protection”, in: Artemi Rallo Lombarte, Rosario García Mahamut (eds), Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime (Tirant lo Blanch, 2015), at 516.
\textsuperscript{296} Federico Ferretti concludes that the balancing under Article 7(f) of Directive 95/46 weakens the protection; see: Federico Ferretti, “Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?”, CMLR 51 (2014), Issue 3, pp. 843-868.
\textsuperscript{297} See Chapter 6, Section 14 of this study.
\textsuperscript{300} Christopher Docksey, “Articles 7 and 8 of the EU Charter: two distinct fundamental rights”, in: Alain Grosjean (ed.), Enjeux européens et mondiaux de la protection des données personnelles (Éd. Larcier, 2015), at 3.
game for processing, or “a sort of Digital Highway Code”. Hustinx asserts that the right to
data protection as laid down in EU law is “intended as a system of ‘checks and balances’ to
provide a structural protection to individuals in a wide range of situations”,301 irrespective of
whether any normative value in a concrete situation is affected.

González Fuster takes a different position302 by explaining that any processing of personal
data constitutes a limitation of the right to data protection under Article 8(1) Charter. The
conditions for the lawfulness of limitations are laid down in Article 8(2) Charter, which
should be read in conjunction with Article 52(1) Charter, the general provision on limitations
of fundamental rights.

This study disagrees with González Fuster on this particular point, in line with the view that
the right to data protection must not be interpreted in line with the right to self-determination.
The study concurs with the position that data protection must be seen as ‘rules of the game’
or ‘a system of checks and balances’, which finds its basis in the wording of Article 8(2)
Charter, as well as Directive 95/46 and other EU instruments for data protection. Under EU
law, an individual has a claim vis-à-vis governments and private actors that his or her data are
processed in an appropriate manner in a system of checks and balances, which is specified in
the Charter as “fairly for specified purposes and on the basis of the consent of the person
concerned or some other legitimate basis laid down by law”303. In Schecke, the Court stated
that Article 8(2) “thus authorises the processing of personal data if certain conditions are
satisfied.”304

However, we must admit that the case law of the Court of Justice does not fully reflect this
position. First, in Schecke, the Court was not entirely consistent. Even though this case relates
to a situation where there is a legitimate basis laid down by law, the Court nevertheless asked
additionally for consent. This additional requirement may be seen as positive in that it gives
an individual an additional safeguard where processing takes place on another legal basis, but
it is not in line with the text of the Charter.305 Second, the Court stated, in Digital Rights
Ireland and Seitlinger,306 that an EU directive constitutes an interference with the right to
data protection, precisely because it provides for the processing of personal data. Possibly,
the Court needed this statement in order to be able to examine the directive under Article

---

Protection Regulation”, published in the “Collected Courses of the European University Institute's Academy of
European Law, 24th Session on European Union Law, 1-12 July 2013”, at 2C.
302 Gloria González Fuster, “Curtailing a right in flux: restrictions of the right to personal data protection”, in:
Artemi Rallo Lombarte, Rosario García Mahamut (eds), Hacia un Nuevo derecho europea de protección de
datos, Towards a new European Data Protection Regime (Tirant lo Blanch, 2015), e.g. at 527-528.
303 Article 8(2) Charter, first sentence.
304 Joined Cases C-92/09 and C-93/09, Schecke (C-92/09) and Eifert (C-93/09) v Land Hessen, EU:C:2010:662,
at 49.
305 Para. 64 of the ruling, as discussed in Peter Hustinx, “EU Data Protection Law: The Review of Directive
95/46/EC and the Proposed General Data Protection Regulation”, published in the “Collected Courses of the
European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July
2013”, at 4D. See also: Christopher Docksey, “Articles 7 and 8 of the EU Charter: two distinct fundamental
rights”, in: Alain Grosjean (ed.), Enjeux européens et mondiaux de la protection des données personnelles (Éd.
Larcier, 2015), at 4b.
306 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), at 36.
52(1) Charter.\textsuperscript{307} In any event, it is not in line with the position that data protection does not prevent processing.

A final remark relates to the application of EU data protection law in horizontal situations. In general, an individual has a claim vis-à-vis governments and private actors. In addition, Article 16(2) TFEU and Article 8(3) Charter provide that data processing is subject to the control of an independent authority. As reiterated by the Court, this is an essential component of the right to data protection\textsuperscript{308}. As part of the claim that individuals have that their data are processed in an appropriate manner in a system of checks and balances they are entitled to control by an independent authority.\textsuperscript{309} Obviously this is a claim they have against governments, not against private actors.

\textit{Summing up: the EU and the Member States must establish checks and balances}

As stated before, the right to data protection not only protects against a government, but also requires active legislative intervention by the same government. However, this does not necessarily mean that the right to data protection – despite its wording (“everyone has the right”) – does not have direct effect.\textsuperscript{310} Although this may be a purely hypothetical question under current EU law,\textsuperscript{311} an answer to this question would clarify the nature of the right to data protection. This may also be of relevance in situations with an extraterritorial effect or in external EU action.\textsuperscript{312}

The doctrine of direct effect, as developed by the European Court of Justice since \textit{Van Gend & Loos},\textsuperscript{313} means that provisions of binding EU law that are sufficiently clear, precise and unconditional can be invoked and relied upon before national courts.\textsuperscript{314} It is arguable that, in the absence of any legislative instrument implementing or specifying Article 16 TFEU and Article 8 Charter and thus in the absence of any other legitimate basis laid down by law, an individual can claim that his or her data can be processed fairly only for specified purposes and with his or her consent. This would also mean, in this hypothesis, that the state should refrain from processing in the absence of consent. Furthermore, it would mean that, under the

\textsuperscript{307} If the right to data protection did not entail any prohibition, but instead provided for checks and balances, how would it be possible to examine limitations of the right in the way foreseen in Article 52 Charter?
\textsuperscript{309} This is one of the most fundamental differences with the legal system of the United States, as will be elaborated in Chapter 7 of this study.
\textsuperscript{311} Member States have implemented Directive 95/46/EC and Council Framework Decision 2008/977/JHA, while outside the scope of these instruments they are bound by Convention 108. The EU institutions are bound by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
\textsuperscript{312} As will be developed in Chapter 9 of this study.
\textsuperscript{314} See also: Paul Craig and Gráinne de Búrca, EU Law, Text, Cases and Material (Fifth Edition), (Oxford University Press, 2011), Chapter 7.
Charter and in the absence of consent, any processing operation lacking a legitimate basis laid down in law would, by definition, be illegal.\textsuperscript{315}

Possibly, the right to data protection would indeed have direct effect, in the absence of a legislative instrument. However, this possibility only makes more evident that EU law requires the European Union (and, where relevant, the Member States) to establish checks and balances in legislative instruments.

Summing up, the position that data protection must be seen as ‘rules of the game’ or ‘a system of checks and balances’ for data processing means that processing of personal data cannot be seen as interference with a fundamental right under Article 52(1) Charter. The right to data protection is respected insofar as the conditions of Article 8(2) Charter are fulfilled, and this requires scrutiny of notions such as fairness and legitimacy. In substance, there is similarity with the proportionality test under Article 52(1) Charter, although this latter test does not serve to determine whether the conditions for data processing are fulfilled, but whether there is interference with a fundamental right. This implies the application of a different test of appropriateness in an information society. To summarise, the test under Article 52(1) Charter is not appropriate, in our view, for data protection.\textsuperscript{316} We find support for this view in the explanation on Article 52(1) Charter by Peers, who states that Article 52(1) sets out rules that apply \textit{if} fundamental rights are limited. Article 8(2) Charter does not contain a limitation of the right to data protection. Hence, Article 52(1) Charter does not apply to the conditions set under Article 8(2) Charter.\textsuperscript{317}

\textbf{13. Privacy and Data Protection: two Sides of the same Coin}

Although not identical, the rights to privacy and data protection – two different rights in the Charter – are closely connected. They can be seen as civil and political rights and as reflecting human dignity. As Hustinx underlines, they are “expressions of a universal idea with quite strong ethical dimensions: the dignity, autonomy and \textit{unique value} of every human being”.\textsuperscript{318}

It was not obvious that the Charter would introduce a fundamental right to data protection in addition to the right to privacy.\textsuperscript{319} Data protection does not appear as a separate fundamental right in other jurisdictions. Even within the Council of Europe, which adopted Convention

\begin{itemize}
\item \textsuperscript{315} Article 52(1) would not change this since it applies only to “any limitation on the exercise of the rights and freedoms recognised by this Charter” (underlining by author).
\item \textsuperscript{316} See also: Gloria González Fuster, “Curtailing a right in flux: restrictions of the right to personal data protection”, in: Artemi Rallo Lombarte, Rosario García Mahamut (eds.), Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime (Tirant lo Blanch, 2015).
\item \textsuperscript{317} Peers and Prechal in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds.), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014), at 52.34. This statement is attributable to Peers.
\item \textsuperscript{319} On this, see: Orla Lynskey, “Deconstructing Data Protection: The ‘added-value’ of a right to data protection in the EU legal order”, International and Comparative Law Quarterly, Volume 63, Issue 03, July 2014, pp. 569-597.
\end{itemize}
108 on data protection, the main protection of personal data is provided by the European Court of Human Rights in its case law on Article 8 of the European Convention on Human Rights on the right to private life.\textsuperscript{320} Moreover, the Explanation on Article 8 of the Charter of Fundamental Rights itself refers not only to instruments of data protection such as Directive 95/46 and Council of Europe Convention 108, but also explicitly to Article 8 ECHR.

A common argument for the introduction of data protection as a separate fundamental right is that it is broader than privacy protection since it also relates to other rights and freedoms\textsuperscript{321} and protects data regardless of their relationship with privacy.\textsuperscript{322} However, the question as to whether data protection is merely a subset of privacy, or delivers additional protection, is open to discussion.\textsuperscript{323} To make it even more ambiguous, the term used in international contexts, and especially in the United States, is data privacy.\textsuperscript{324}

In its case law, the Court of Justice does not make a systematic distinction between privacy and data protection.\textsuperscript{325} In \textit{Schecke},\textsuperscript{326} the Court referred to both rights at the same time, and also did the same in \textit{Schwarz}, while affirming this as a “joint reading”.\textsuperscript{327} In \textit{Digital Rights Ireland and Seitlinger},\textsuperscript{328} the Court mentioned the relationship between Articles 7 and 8 Charter on various occasions. The retention of data “directly and specifically affects private life, but it also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article.”\textsuperscript{329} The Court also mentioned the important role of data protection in the light of the fundamental right to privacy.\textsuperscript{330} \textit{Schrems} also addressed both fundamental rights jointly, sometimes in a general context of fundamental

\begin{footnotes}
\footnote{This fairly cautious wording has been chosen since the ECtHR is not used to referring directly to Convention 108. See: G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2014, at 4.3.}
\footnote{The preamble of Convention 108 states: “Considering that it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy” (underlining by author). Similar wording can be found in all EU instruments on data protection.}
\footnote{Kokott and Sobotta in: Hielke Hijmans and Herke Kranenborg (eds), Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014) (Antwerp: Intersentia, 2014), at 83. See also: Orla Lysnkey, “Deconstructing Data Protection: The ‘added-value’ of a right to data protection in the EU legal order”, International and Comparative Law Quarterly, Volume 63, Issue 03, July 2014, pp 569-597; Lysnkey points to the failure to provide a convincing rationale for including the right to data protection in the Charter.}
\footnote{In addition, the leading legal journal in the area (UK-based) is called International Data Privacy Law.}
\footnote{See also: Herke Kranenborg in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), The EU Charter of Fundamental Rights, A Commentary (Hart Publishing, 2014), at 230; Gloria González Fuster, “Curtailing a right in flux: restrictions of the right to personal data protection”, in: Artemi Rallo Lombarte, Rosario García Mahamut (eds), Hacia un Nuevo derecho europeo de protección de datos, Towards a new European Data Protection Regime (Tirant lo Blanch, jaar), at 522-524.}
\footnote{Joined Cases C-92/09 and C-93/09, \textit{Schecke and Eiffert v Land Hessen}, EU:C:2009:284.}
\footnote{Case C-291/12, \textit{Schwarz}, EU:C:2013:670, at 25.}
\footnote{Joined Cases C-293/12 and C-594/12, \textit{Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)}.}
\footnote{Para. 29 of the ruling.}
\footnote{Paras 48 and 53 of the ruling. The CJEU follows the – stronger – formula of the ECtHR that the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life (e.g., Z v \textit{Finland}, 1997, Application No 22009/93, at 95).}
\end{footnotes}
rights protection and in relation to effective legal protection under Article 47 Charter. In short, although the Court mentioned Article 7 in some paragraphs, Article 8 in others and both articles in yet other paragraphs, a clear line cannot be drawn from this approach. The absence of this clear line is confirmed by Deutsche Telekom, where the Court referred only to Article 8 Charter and by Ryneš, where the Court referred only to Article 7 Charter.

Another case that demonstrates that the Court of Justice does not make a systematic distinction between privacy and data protection is Commission v Bavarian Lager. This case concerned a problem in the specific context of public access to documents of EU bodies containing personal data. The case related to the documents with lists of participants in professional meetings. The distinction between privacy and data protection was at the heart of the proceedings. The Court had to decide on an appeal by the Commission against a decision of the Court of First Instance (now: General Court) where – in this specific context – such a distinction was made. The Court of First Instance explicitly stated that not all professional activities of an individual are wholly and necessarily covered by the right to privacy. At stake was the interpretation of Article 4(1) of Regulation 1049/2001 on public access to EU documents, which reads as follows: “The institutions shall refuse access to a document where disclosure would undermine the protection of […] privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.” The main question was whether the wording “undermine the protection of privacy and the integrity of the individual” had an autonomous meaning because privacy represented an extra threshold in addition to data protection, or whether the said article simply meant to refer to the data protection legislation, which would imply that privacy equals data protection. The Court of Justice upheld the appeal against the decision of the General Court, and by doing so did not attach added-value to the mentioning of privacy.

The Court has been criticised for not properly distinguishing between privacy and data protection. This criticism contains *grosso modo* two elements. In the first place, the case

---

332 Case C-543/09, Deutsche Telekom, EU:C:2011:279, at 49-54.
334 In Case C-473/12, IPI, EU:C:2013:715, the CJEU admittedly does not mention the Charter at all.
338 And integrity, but the latter was of no further relevance in this specific case.
law does not reflect the broad scope of the right to data protection exceeding the scope of privacy, while, in the second place, it does not reflect the nature of the right to data protection because it is based on the interference of the right instead of on the conditions for processing.  

341 It is not important to distinguish between privacy and data protection on the internet

The preceding sections show that privacy and data protection are different concepts. The right to privacy represents a normative value, whereas the right to data protection represents a legal structure aimed at allowing individuals to claim that their data should be fairly and lawfully processed.  

Privacy can be depicted as a principle-based right, and data protection as a rule-based right.  

We have also seen that, in the case law of the European Court of Human Rights and the Court of Justice of the European Union, the right to privacy has been broadly interpreted and is not confined to the right to be left alone as it extends to areas outside the private sphere. In its broad interpretation it is closely linked to other fundamental rights concerning human dignity, such as the freedom of expression. Where the right to privacy implies the notion of autonomy, it is close to data protection. Indeed, the case law of the Court of Justice does not make a systematic distinction between these two fundamental rights. Moreover, as explained above, the concepts used in the international context are informational privacy or data privacy, which contain at least the main elements of both rights.

Against this background we raise the issue of the importance of the distinction, while being fully aware that privacy and data protection are not identical concepts, and that the Charter contains two fundamental rights. More precisely, we submit the following points for consideration.

First, we have seen that privacy and data protection are values that matter and that are being challenged in an information society. Privacy as a concept is difficult to capture in precise terms, and data protection – as a system of procedural checks and balances – could provide the necessary grip for ensuring effective protection.

Second, the differences in scope between privacy and data protection have been emphasised by various authors. Data protection is both more specific than privacy, because it only protects personal data, and also wider because it protects all personal data, also in relation to other fundamental rights such as the right to non-discrimination.  

However, the relevance of

341 As explained in Section 11 above.
342 This would also concur with the developments in the United States in the 1970s, where principles on data privacy were developed, focusing on efficiency rather than on normative values; see: James Rule, Douglas McAdam, Linda Stearns, David Uglow, The Politics of Privacy, Planning for Personal Data Systems as Powerful Technologies (New York: Elsevier, 1980).
343 This is the distinction used by Barak when he deals with conflicting constitutional rights; see: Aharon Barak, Proportionality; Constitutional Rights and their Limitations (Cambridge University Press 2012), Chapter 3.
344 As will be explained in more detail in Chapter 5.
distinguishing between the right to privacy and the right to data protection has faded due to the increased importance of informational privacy, as well as the broad scope of privacy in an information society extending to the public sphere.

Third, the method of assessment by the European Court of Justice is not fully satisfactory. In its case law, the Court does not make a clear distinction between the two rights, and this may lead to partially overlapping assessments and, as a consequence, to legal uncertainty. Moreover, Article 8 Charter comprises a system of check and balances that cannot be meaningfully scrutinised under Article 52(1) Charter, given that the former contains conditions for processing, not a prohibition on processing that can be justified in accordance with the restrictions under Article 52.

A further argument for not distinguishing between privacy and data protection: the law of the United States

The case law of the US Supreme Court on the constitutional right to privacy\(^{346}\) acknowledges the existence of such a right to privacy, as a sort of accessory right to the fundamental rights protected under the US Bill of Rights. Privacy deserves protection within the scope determined by these other rights. The Supreme Court states that the specific guarantees in the Bill of Rights have penumbras.\(^{347}\) The Court declared in Roe v Wade that the “right of privacy, whether it be founded in the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action, as we feel it is, or, as the district court determined, in the Ninth Amendment’s reservation of rights to the people, is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy.”\(^{348}\)

However, the US Supreme Court denies the existence of a general right to privacy under US federal law. The Fourth Amendment\(^{349}\) protects certain elements of the private sphere of individuals against unreasonable intrusion by government, in particular against unreasonable searches and seizures, but, as confirmed in the landmark case Katz v United States (1967),\(^{350}\) "The Fourth Amendment cannot be translated into a general constitutional ‘right to privacy’. […] [This] right to privacy – his right to be let alone by other people – […] [is] left largely to the law of the individual States." The US Supreme Court created in Katz v United States the notion of a constitutionally protected reasonable expectation of privacy,\(^{351}\) a notion that is used in a large number of contexts, also within the European Union.

---

346 See also: G. González Fuster, “The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Law, Governance and Technology Series 16, 2.1.2.
347 E.g., Griswold v Connecticut, 381 U.S. 479 (1965), on privacy and a marital relationship, and the famous case Roe v Wade, 410 U.S. 113 (1973), on the right to abortion.
349 Full text: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
351 In a concurring opinion in this case by Justice Harlan.
A constitutional right to data protection does not exist in the US, and although the term ‘data protection’ may be used, the more common term is ‘data privacy’ or ‘informational privacy’ thus illustrating that this is not a legal notion that can be considered separately from the right to privacy.

14. **A Proposal for a Solution considering both Fundamental Rights as Part of one System**

Instead of distinguishing the closely related rights to privacy and data protection, should we perhaps not consider both fundamental rights as part of one system, whereby the right to privacy – in its broad meaning – represents the value that requires protection (why protection is needed) and the right to data protection the structure of protection (how protection is delivered)?

This solution would mean, more concretely, that the structures of data protection as laid down in Article 8(2) Charter and further specified in secondary law based on Article 16(2) TFEU would be instrumental to the right to privacy. Data protection rules should ensure that privacy can be delivered. Arguably this is exactly what the Court of Justice said in *Commission v Bavarian Lager*.

Under this proposal, the test of compatibility with the Charter would be based on Article 8 Charter, not on Article 7. The test would be whether the requirements of data protection are fulfilled. As part of the test of the fairness and lawfulness of data processing, the European Court of Justice could analyse the interference of the right to privacy. This includes not only the interference itself, but also the justification and proportionality.

Since the Court of Justice deals with cases on the interpretation or validity of secondary law and not on the interpretation of the Charter itself – at least that has been the practice until now – the proposed approach will provide an appropriate structure for assessing secondary law in the light of the fundamental rights of Article 7 and 8 Charter. While the right to privacy under Article 7 Charter potentially extends to all uses of personal information on the internet, the system of checks and balances foreseen in Article 8 Charter must deliver effective, but at the same time proportionate protection. This would enable the Court to deal

---


353 Or, in the words of the CJEU, “the protection of personal […] is especially important for the right to respect for private life”, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*, EU:C:2014:238, at 53.

354 This is also in line with the distinction between principle-based rights and rule-based rights, as used by Aharon Barak, *Proportionality; Constitutional Rights and their Limitations* (Cambridge University Press, 2012), Chapter 3. Privacy falls within the first category, data protection within the second category.

355 Inspiration is found in Gloria González Fuster, “Curtailing a right in flux: restrictions of the right to personal data protection”, in: Artemi Rallo Lombarte, Rosario Garcia Mahamut (eds), *Hacia un Nuevo derecho europeo de protección de datos*, Towards a new European Data Protection Regime (Tirant lo Blanch, 2015), at, e.g., 519. González Fuster follows a different reasoning, but argues extensively that Articles 7 and 8 Charter are combined. She qualifies Directive 95/46 (and Regulation 45/2001) as containing conditions and limitations for the right to privacy with regard to the processing of personal data.

356 As will be explained in Chapter 5.
with the provisions more logically as it could then examine cases in a more structured manner by scrutinising whether the requirements of data protection are fulfilled. Moreover, the checks and balances included in data protection law could give practical meaning to reasonable expectations of privacy.

This approach would have several advantages as it would allow us to end the semantic discussion on the differences between privacy and data protection. It would fully recognise the different nature of the rights, as discussed by Hustinx and others, whereby Article 8 Charter serves as a provision specifying the safeguards for delivering privacy. In our view, this approach will not unduly limit the scope of Article 16 TFEU, and the rules adopted on this legal basis, to cases where privacy is involved, given that Article 16 TFEU provides an autonomous and wide legal basis and also mentions the free movement of data.

This approach would also bring the European Union more into line with the international debate, where no distinction is made between privacy and data protection. This alignment with the international debate would facilitate the negotiating position of the Union and allow it to concentrate in international fora on the substance of the protection. Furthermore, this approach would contribute to global solutions and simplify the discussions on extraterritorial application of EU law.

Admittedly, this approach does not reflect the views of those who consider data protection to be a much broader notion than privacy since it goes beyond what is ‘private’. Docksey, for example, makes a distinction between what is personal and what is private. He refers in this context for instance to Österreichischer Rundfunk and others, where the Court of Justice ruled that the mere recording of employee data does not constitute interference with the right to privacy under Article 8 ECHR, whereas communication of these data to others does constitute such interference. Apparently there is – or at least there was, as this case dates from before the Lisbon Treaty – a domain where data protection rules apply outside the scope of privacy.

This leads to the argument submitted by this study as decisive. The distinction between privacy and data protection no longer makes any sense in the era of big data, where all personal data processing potentially affects privacy in the broad sense, as recognised in the case law of the European Court of Human Rights and the Court of Justice of the European Union. Moreover, by combining Articles 7 and 8 Charter, the Court of Justice has arguably adopted a different approach since the entry into force of the Lisbon Treaty.

15. Conclusions

Privacy and data protection are constitutional values that matter in a networked information society. However, the internet is resulting in a substantive increase in the use of massive amounts of data and a loss of control over these data. This may create substantive risks, both

---

357 As well as other fundamental rights.
358 Case C-465/00, Österreichischer Rundfunk and others, EU:C:2003:294, at 73-74.
for individuals and for our democratic societies, if not accompanied by effective and legitimate rules that counterbalance the undesired effects.

This chapter explained general features of the rights to privacy and data protection, and more specifically when respect for privacy and data protection is needed on the internet. The entitlement of individuals to full privacy and data protection generates a duty for the European Union and national governments within the scope of EU law to ensure protection, even with regard to a first-generation fundamental right, as is definitely the case with the right to privacy in Article 7 Charter. Fulfilment of this duty is needed to promote democracy and, even more directly, the rule of law in its essential fashion as this “requires as a minimum that the law actually rules”. For data protection, the duty to protect this fundamental right is laid down in Article 16 TFEU.

A general design of privacy and data protection as part of a European Union based on values starts with the high ambitions of the Union in promoting its values, particularly democracy, the rule of law and fundamental rights. These three values are inextricably linked. These values are shared between all the Member States and represent the premise of mutual trust among the Member States themselves and between the Member States and the Union (Section 2).

Privacy and data protection are constitutional values that matter, also on the internet, although people value the seriousness of privacy breaches in diverging ways. Greenwald gives two convincing arguments for privacy and data protection: there are no good and bad people, and monitoring changes behaviour. The effect of breaches of these rights are summarised, firstly, as a lack of control over information, thus hampering the autonomy of individuals, and, secondly, as full transparency of individuals and their behaviour, thus hampering their dignity (Section 3).

The European Union has ambitions in promoting democracy. A free internet is needed, but not an unprotected internet. A free internet empowers individuals to share information in an unprecedented way and boosts democracy. Although governments must in principle abstain from intervention, there are certain situations in which they should also actively ensure democratic rights, particularly internet privacy and data protection. Democratic governments must also protect society against threats, including those caused by serious crime and terrorism (Section 4).

The European Union has ambitions in promoting the rule of law. The rule of law in its essential fashion, whereby it “requires as a minimum that the law actually rules”, is not always respected. Under the rule of law, there must be order in society and control of power, and everyone is entitled to effective legal protection. There is a close link between the rule of law and data protection. The (lack of) effective redress on the internet is a main theme in privacy and data protection (Section 5).

359 One could argue that a similar obligation already exists under Article 1 ECHR, whereby the High Contracting Parties – which include all EU Member States – “shall secure to everyone within their jurisdiction the rights and freedoms […].”

360 As explained in Section 5 above, based on Armin von Bogdandy, Michael Ioannidis, “Systemic deficiency in the rule of law: What it is, what has been done, what can be done”, CMLR 51, Issue 1, pp. 59-96, at 63.
The European Union also has ambitions in promoting fundamental rights, which are broadly applicable. In an internet context, this entails individuals being entitled to the protection of fundamental rights when they are active on the internet (online), in the same way as when they are acting in any other capacity (offline). Moreover, the external dimension – protection vis-à-vis actors in third countries – has an increased weight. However, individuals are not entitled to protection against all risks on the internet, and there is no zero-risk approach (Section 6).

Fundamental rights protection in horizontal relations acquires a new dimension on the internet. However, the impact of the Charter is not fully clear in this respect. The following arguments support the applicability of privacy and data protection in horizontal relations on the internet: the Charter is part of EU law; the case law recognizes the horizontal applicability of certain provisions of the Charter, and data protection aims to prevent possible misuse of personal information in the private sector, also in view of the dominant position of big internet companies (Section 7).

The right to privacy is a broad and dynamic concept on the internet, extending to the public sphere. Human dignity and personal autonomy are underlying values. Privacy has a broad scope, but in the view of the European Court of Human Rights and the Court of Justice it does not encompass all use of personal information. This study challenges this limitation of scope. On the internet, the distinctions between the private sphere and the public sphere are blurring, while one cannot know in advance how data will be used in the era of big data (Section 8).

Privacy can be understood by looking at qualified interests: information is used by governments, health data are revealed, vulnerable groups are identified and reputations are lost. This study argues that qualified interests are not a condition for bringing the use of personal data within the scope of privacy, but rather they determine the assessment of any interference of this right. Two reasons support this argument: the Court of Justice does not make a systematic distinction between privacy and data protection, and all processing of personal data on the internet potentially affects privacy (Section 9).

The right to data protection developed as a response to technological developments. Directive 95/46 had a double objective of promoting an internal market of personal data and protecting the individual. The inclusion of data protection in Article 16 TFEU and in Article 8 Charter implies a change in the centre of gravity of data protection, towards fundamental rights protection. The developments in the area of freedom, security and justice confirm this change (Section 10).

The right to data protection is a claim based on fairness and provides safeguards where personal data are processed. This study argues that data protection is not based on the right to informational self-determination, which gives the individual a right to prevent the processing of personal data. There is no right to prevent processing. This is the result of how the European Court of Justice emphasises the balancing of various interests, and the result of the internet, with big data and the processing of personal data by search engines without consent as examples. The emphasis on fairness should not result in weak protection (Section 11).
Data protection constitutes ‘the rules of the game’ or ‘a system of checks and balances’. The underlying value is not important. The right is respected when the conditions of Article 8(2) Charter are fulfilled; this should be scrutinised in a test under Article 8(2) Charter. In substance, this test is similar to a proportionality test under Article 52(1) Charter, although the test should not serve to establish whether there is interference with a fundamental right, but instead whether the personal data have been fairly processed according to the conditions laid down in Article 8(2) Charter and in secondary EU law. Since the test under Article 52(1) Charter is not appropriate for data protection, the information society needs this new kind of testing (Section 12).

Privacy and data protection are two sides of the same coin, both reflecting human dignity. The right to privacy represents a normative value, while the right to data protection represents the ‘rules of the game’. It is not important to distinguish between privacy and data protection on the internet, due to the growing importance of informational privacy, and the broad scope of privacy extending to the public sphere. The European Court of Human Rights and the Court of Justice of the European Union interpret privacy broadly, and the latter does not make a systematic distinction between the two fundamental rights (Section 13).

This study proposes, instead of distinguishing the closely related rights to privacy and data protection, to considering both fundamental rights as part of one system, whereby the right to privacy – in its broad meaning – represents the value that requires protection (why protection is needed), while the right to data protection represents the structure of protection (how protection is delivered). The proposed approach provides a structure for the assessment of secondary law in the light of the fundamental rights of Articles 7 and 8 Charter. The approach reflects the reality in the era of big data, where all personal data processing potentially affects privacy (Section 14).

This proposal allows an approach whereby the Court of Justice of the European Union could examine cases on privacy and data protection in a more structured manner by scrutinising whether the requirements of data protection are fulfilled. As part of the test of the fairness and lawfulness of data processing, the Court could analyse interference of the right to privacy.
Chapter 3. Internet and Loss of Control in an Era of Big Data and Mass Surveillance

1. Introduction

This study starts from the perception that the online environment is different from the physical world and that on the internet, as a global network with a loose government structure, control over personal data has been lost. However, individuals remain fully entitled to full protection of these fundamental rights. Where control is lost, control needs to be regained. It is the responsibility of governments, be it the European Union or national governments, to deliver this result.

This chapter describes certain developments in the internet economy and in communications on the internet that affect the safeguarding of privacy and data protection of individuals, with a focus on big data and mass surveillance, and identifies challenges for privacy and data protection on the internet. It provides a further element for answering the general part of the research question: “How does the constitutional mandate under Article 16 TFEU contribute to legitimate and effective privacy and data protection on the internet.” This chapter includes the following subjects:

a. the general design of the internet and the loss of control over personal data;

b. the internet as a single unfragmented space with a loose government structure, and networked societies;

c. big data justifying a qualitative shift in thinking;

d. surveillance that people cannot avoid;

e. the changed perspective of the European Union and the Member States;

f. introductory ideas how to regain control.

The first objective of the chapter is to demonstrate that our societies are changing in a fundamental way, affecting privacy and data protection. The second objective is to clarify the perspective of the European Union and national governments: which changes are they faced with and what are the directions for regaining control?

Section 2 introduces the information society in relation to the loss of control over personal data. Section 3 elaborates on the internet as a single unfragmented space with a loose governance structure, outlining four dimensions of the internet economy, largely based on Castells’ work. Various tendencies point at a fragmentation of the internet: Section 4 discusses the question to what extent this poses a threat. Commentators observe a shift on the

---


internet from freedom for all to powers of a few. Section 5 depicts power as a complex matter and then focuses on a specific power, the power of the EU, to effectively protect its values.

Subsequently, the chapter focuses on two specific themes that pose main challenges to the effective protection of constitutional values, and in particular to the fundamental rights of privacy and data protection. The first theme is big data (Section 6), which justifies a qualitative shift in thinking about the collection and use of information in an information society. The second theme is surveillance through electronic means (Sections 7-8), distinguishing between surveillance by states and by private companies, between mass surveillance and targeted surveillance and, a topic relevant for surveillance by states, between internal and foreign surveillance.

Section 9 takes the perspective of the European Union, and its Member States, faced with developments in the internet economy and communications on the internet, and discusses main areas substantially affecting competences. Section 10 introduces general directions for addressing these issues. These sections can be seen as the bridge with the remainder of the study, which focuses on the mandate of the Union itself. Section 11 contains conclusions.

The ambition of this chapter is limited: it deals with the protection of constitutional values on the internet. The internet economy’s main features and developments in internet communications are described in an abstract way to avoid these sections becoming obsolete when new technology emerges.

The chapter is based on sources that enjoy a wide recognition in the debates on internet developments, including – where relevant – short arguments of what commentators regard as the most imminent threats to the functioning of the internet. It is meant to be illustrative, not exhaustive. This also explains the choice for big data and mass surveillance as central themes. This choice could have been different and could also have included internet security as main theme.363

2. A General Design of the Internet and the Loss of Control over Personal Data

At the start of the 2009 edition of his Rise of the Network Society Castells observes: “We live in confusing times, as is often the case in periods of historical transition between different forms of society. This is because the intellectual categories that we use to understand what happens around us have been coined in different circumstances, and can hardly grasp what is new by referring to the past.”

363 Svantesson for instance includes security difficulties as significant change in the online environment; see: Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing 2013, at 46.
This chapter describes what the European Commission identifies as motive for the reform of the data protection framework in the EU: the rapid pace of technological change and globalisation, leading to a new online environment. The new online environment is also known as the information age, the network society or the information society. These qualifications capture the essence of societal developments and have also triggered this study on privacy and data protection on the internet.

The information society, or the information age as Castells calls it, is a period of unprecedented technological change, both in terms of the extent and speed of change. The essence of the change is not the technology itself, but the diffusion of technology in society and the fundamental changes in society it causes. The internet itself provides the classical example to explain this: while internet technology was first deployed in 1969, it was only in the 1990s that it was widely diffused and started to have a significant impact on societies, also due to other developments, such as the wide-scale deregulatory movements and globalisation of markets.

The internet is a global structure with loose. In this digital environment governments lack sufficient means to ensure effective protection of constitutional values, such as the rights to privacy and data protection. This chapter characterises the main features of the internet and developments in communications on the internet on the basis of the concept of the internet as a Networked Society as described by Castells: an environment with an open and globalised structure where the influence of governments is initially limited. This environment has created freedom for individuals, but it also complicates the power of governments where they have to fulfil their legitimate tasks in protecting their citizens.

This double-faced tendency on the internet of creating societal benefits on the one hand while leaving the protection of fundamental constitutional values at least ineffective may be illustrated by two phenomena of concern to privacy and data protection. The first phenomenon is big data, a broad term for data sets so large or complex that...
concepts of data processing are inadequate. The use of big data has significant benefits for society, since it “allows to crunch a vast quantity of information, analyse it instantly and draw sometimes astonishing conclusions from it”. However, the evolving era of big data makes the loss of control over personal information as such visible.

The other phenomenon, mass surveillance by governments and private companies, demonstrates the impact on the fundamental rights of individuals. The Court of Justice of the European Union underlined the intrusiveness of surveillance in Digital Rights Ireland and Seitlinger: it is “likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance”. Surveillance, in particular, is problematic, since the internet is supposed to be a place where individuals should be able to express themselves anonymously, make mistakes and explore their identities.

These two phenomena deserve particular emphasis, because of the direct impact on the mandate of the European Union to ensure privacy and data protection. They are the phenomena giving evidence of the loss of control of individuals over their personal data and of the capability of governments to deliver protection. Privacy and data protection is described in this study as an essential domain where the role of government is or should be undisputed.

Big data and mass surveillance are difficult to reconcile with the mandate of the European Union under Article 16 TFEU in the area of privacy and data protection. As argued by Prins, in our complex and rapidly evolving societies – with an ever greater role of technology – governments lack overview, resulting in loss of control. Governments therefore are not fully able to guarantee the respect of constitutional values. Respect of these values is needed, for the citizens, who are entitled to protection, and for the governments themselves, to be credible and to earn or regain necessary support. Citizens must be able to trust their governments, if only for the benefit of a well-functioning democratic society.

3. The Internet as a Single Unfragmented Space with a Loose Governance Structure

374 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 37.
375 This is connected to the argument in this study that privacy remains important in the information society. See mainly Chapter 2, Section 3.
Interconnected and loosely governed by multiple stakeholders

The internet as we know it is a global system of interconnected computer networks that use the standard internet protocol suite (TCP/IP) to link several billion devices worldwide.\(^{377}\) The strength of the internet lies in its open, distributive nature based on non-proprietary standards, which create low barriers of entry.\(^{378}\)

The internet is also structured as a single unfragmented space, functions without structural governmental or intergovernmental oversight and is governed on the basis of what is called a multi-stakeholder approach: participants in internet governance include representatives of national governments, international organisations, the business sector, civil society and the technical community.\(^{379}\) The multi-stakeholder approach reflects the idea of governance through civil society.\(^{380}\) This non-governmental emphasis in the governance of the internet is one of its strengths, also from a fundamental rights perspective. It is a means to boost democracy and preclude censorship and information control by governments.\(^{381}\) Schmidt & Cohen speak about the internet as the largest experiment involving anarchy in history, the world’s largest un governed space.\(^{382}\)

In this multi-stakeholder approach, which includes involvement of private companies, civil society and governments, several organisations play a role in governance: the Internet Governance Forum, the Internet Corporation for Assigned Names and Numbers (ICANN, founded in 1998), the Internet Assigned Numbers Authority (IANA),\(^{384}\) which is a department of ICANN, and a number of other formal or informal organisations such as the World Wide Web Consortium (W3C), which develops protocols and guidelines, must ensure the long-term growth of the web.\(^{385}\)

The Internet Governance Forum was established by the World Summit on the Information Society in 2006. The forum positions itself as the leading global multi-stakeholder forum on public policy issues related to internet governance. The Internet Governance Forum is

\(^{377}\) Wording taken from Wikipedia; see: https://en.wikipedia.org/wiki/Internet. See also: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance – Europe’s role in shaping the future of Internet Governance, COM/2014/072 final.

\(^{378}\) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance – Europe’s role in shaping the future of Internet Governance, COM/2014/072 final, at 1.


\(^{383}\) An overview can be found in: Jovan Kurbalija, Introduction to Internet Governance (6th Edition), (plaats: DiploFoundation, 2014).

\(^{384}\) According to its website, IANA is responsible for coordinating some of the key elements that keep the internet running smoothly, in particular domain names, number resources and protocol assignments.

endorsed by the United Nations and is a forum for discussion. The Forum does not adopt binding decisions or resolutions.  

ICANN is an independent organisation established in California that coordinates the use of unique internet addresses around the world. It operates on the basis of a Memorandum of Understanding with the US Department of Commerce. For this reason there is criticism that although ICANN is non-governmental, it is nevertheless closely linked to the government of the United States.

A recurring issue in the international debates around ICANN is whether ICANN only should deal with technical problems or also with issues having public policy relevance. An example of interference with policy issues was the admissibility of domain names, exclusively for adult materials. Either solution – admitting these specific domain names or refusing them – is not just based on neutral, technology driven considerations. Another example is the current discussion on the supervision of the assignment of numbers and domain names by IANA. The assignment of numbers and names is not purely a neutral, technical activity either and there is a discussion in ICANN to involve the International Telecommunication Union (ITU), an agency of the United Nations. These examples show that it is difficult to deal with internet governance, without interfering with public policy or with fundamental rights.

Other examples of the public policy nature of internet governance are net neutrality, as well as the necessary policies on privacy and data protection that need to be implemented by the organisations assigning domain names. In these domains, leaving governance to civil society raises questions relating to representation (“who represents civil society?”) and to a likely democratic deficit since core tasks of governments are executed by private parties outside government responsibility, with agendas being set with little regard for public rationale or justification, as Mazower explains. Internet governance is an illustration of why the democratic legitimacy and accountability is a prominent theme in this study.

Responsibility for the integrity of the system, the continuity of the services and security threats

The dependency of the economy, society and individuals on the internet and essential internet-based services like search engines qualifies the internet – or in any event core elements of the internet – as a global public good. This justifies a task for the state in

388 Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De publieke kern van het internet, Naar een buitenlands internetbeleid, Amsterdam 2015, at 33.
390 Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De publieke kern van het internet, Naar een buitenlands internetbeleid, Amsterdam 2015, at 33.
maintaining and establishing the integrity of the system and the continuity of the service, as a prerequisite for the accomplishment of other government roles. Additionally, the internet and internet-based services might possibly qualify as services of general economic interest that are subject to specific public services obligations. Under Article 36 Charter, the European Union recognises and respects access to these services. There is no definition under EU law of services of general economic interest, since this is “regarded as a dynamic and evolutionary concept, especially as technology develops”. Examples of these services are banking services, broadcasting and electronic communications. EU law in the field of electronic communications provides for a social safety net, where market services do not deliver affordable access. A similar safety net does not exist to ensure the availability of internet services.

A related reason for involving governments in internet governance are the growing concerns in relation to cybersecurity, with the result that cybersecurity has become a subject of policies, comprising critical information infrastructure protection (CIIP), cybercrime and cyberconflicts. As to cybercrime, this is a subject for government intervention under the Council of Europe Convention on Cybercrime (2001). Also cyberwarfare – by services of national governments – may paradoxically require involvement of governments or international organisations in internet governance.

Obviously, all these concerns have consequences for the role of governments in the governance structure of the internet and essential internet services. On the one hand, the internet has a societal function that is difficult to reconcile with the position of the internet as the largest experiment involving anarchy in history. On the other hand, too much

---

393 This is the essence of a report of the Scientific Council for Government Policy in the Netherlands; see in Dutch: Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De publieke kern van het internet, Naar een buitenlands internetbeleid, Amsterdam 2015.
399 As explained by Eric Schmidt and Jared Cohen in The New Digital Age (Hodder & Stoughton, 2014), at 103-120, using the term ‘code war’, instead of cold war.
401 As mentioned above, referring to Eric Schmidt, Jared Cohen, The New Digital Age (Hodder & Stoughton, 2014), at 3.
government involvement in the public infrastructure of the internet risks creating barriers to the free flow of information across the globe.402

4. At the Core of the Internet, Networked Societies and Globalisation: Is Fragmentation a Threat?

The information society consists of Networked Societies, or, depending on the definition, of a network society. According to Castells a network society is a highly dynamic, open structure that is susceptible to innovation,403 and in which information is the key ingredient. The development of the internet into a global communication and information network that positions itself mainly outside traditional frameworks and the influence of governments is related to the world we live in, a world composed of networked societies on a local, a regional as well as on a global level. The fact that the internet has developed into a global network is supported widely, because on the one hand it allows innovations that for instance lead to a free flow of information and more democratisation in society,404 whereas on the other hand it precludes – or at least complicates – censorship.405 This is why internet freedom enjoys wide support, also amongst governments.406

The transformation of communication may be the most important social change, as Castells states.407 Although he also mentions the explosion of wireless communication, the most significant transformation is probably what he conceptualised as ‘mass self-communication’. Anyone can reach a potentially global audience through networks, communication is easily accessible408 and it gives power to the individual who can by himself generate content, direct emissions and select reception, while notions of time and space change as well. This potential of the internet is also a tool for democratic participation. Individuals can easily share information on a massive scale, for instance through social media platforms, thus diminishing the dependency on traditional mass media. This is important to Greenwald who claims that the traditional media (at least in the US) were not willing to publish on certain issues relating

408 Castells uses the term ‘multimodal’, meaning that content as well as advanced social software are easily accessible and can easily be reformatted.
to mass surveillance as revealed by Edward Snowden. More people can assume the function of watchdog of governments and play a role in setting the political agenda. Moreover, governments can no longer control information. Information sharing by individuals was an important enabler of democratic changes in the Arab world in 2010.

From the perspective of individuals, one can observe a development in society where the difference between what happens online and what happens offline becomes less relevant. Connectivity becomes an increasing part of our daily lives: not only are individuals permanently connected through mobile devices, but also through phenomena like the Internet of Things. A variety of devices varying from medical devices to household appliances become internet-enabled. Users seem to have a widespread trust in the companies that process their data. The sharing of large amounts of personal information on social media is just an example of this trust.

*Networked societies are vulnerable*

Major threats are the consequence of an intentional or unintentional loss of security on the internet. In a special issue, The Economist notices that criminal hackers have multiplied, become more professional posing significant threats to internet companies. Combating these types of cybercrime is complicated, also because cybercrime often involves multiple jurisdictions. Moreover, there are unintentional losses that adversely affect cybersecurity. The Economist reports an exponential growth of data breaches, up to 800 million records in 2013. Many of these breaches were caused by deliberate attacks.

These are obvious risks in the information society, if only because the internet was designed to promote connectivity, not security and become even more prominent in view of the dependency of individuals in the information society on electronic communications and their permanent connectivity through mobile devices. Further risks for security relate to the expected integration of the Internet of Things in the lives and homes of individuals, be it webcams monitoring small children, wearable medical devices or smart fridges.

---

411 The Arab spring, see on this in Dutch: Adviesraad Internationale Vraagstukken (AIV), Advies 92, Het Internet: een wereldwijde vrije ruimte met begrensde staatsmacht, November 2014, at 64.
412 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Internet of Things: an action plan for Europe, COM/2009/0278 final.
413 See examples by Bruce Schneier, *Data and Goliath* (W.W. Norton & Company, 2015), at 15-17.
416 E.g., this dependency played a role in the decision of the CJEU leading to the invalidity of Directive 2006/24, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*, at 27.
A lot can be said about the security threats for the internet as such and for the protection of personal data on the internet. Security of personal data is an essential and inherent element of the system of data protection, as confirmed by the European Court of Justice and illustrated by the EU legal instruments on data protection. Examples of those instruments are Article 17(1) of Directive 95/46 on data protection requiring that a data controller implements appropriate technical and organisational measures to protect personal data and the provisions on the notification of personal data breaches. Under current EU law, the notification of personal data breaches is an obligation for providers of publicly available electronic communications. For this study, which adopts the perspective of the European Union acting as guardian of privacy and data protection, it suffices to keep in mind that, in the information society, the threats to security are significant.

Globalisation, a trigger for innovation and growth

Globalisation, a development where key components of our economy are organised on a global scale, is a further dimension of the information society. Globalisation is seen as a trigger for innovation and growth, based on a belief in the efficiency of markets. This is a reason why governments in general embraced globalisation.

The internet is a testimony of globalisation, due to its globalised and in essence unfragmented infrastructure where information is exchanged and accessible worldwide. The whole internet is, in principle, accessible for anyone who connects to it, although some national laws contain restrictions and some content is blocked as a result of licensing agreements. Also search engines make distinctions depending on national or regional borders.

---

419 In particular: Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 40. See also Chapter 5, Section 17 of this study.
421 E.g., Article 17(1) of Directive 95/46 reads: “Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.”
423 As announced in Chapter 1, the subject of this study is not internet security.
427 This differentiation was an essential feature in Case C-131/12, Google Spain and Google Inc., EU:C:2014:317. See also The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015.
In principle however, the internet is of a global nature, not limited to specific territories, nor bound by national borders. This global nature is widely seen as an added value to society, because it is an effective means of bringing people together. We discussed this already in Chapter 2, adding that the result may not be that the internet is an unprotected zone where governments and regional governmental organisations such as the European Union, both based on physical territories, lack effective intervention to protect individuals.

On the internet, information does not only flow over the whole world, but in many situations information is not under the control of one specific party. The case of Google Spain and Google Inc. is an example where an individual challenged the publication of certain personal data not only against the publisher of this information, but also against a search engine that had facilitated the access to this information and against a European establishment of the search engine using this information for commercial purposes. However, this is still a simple case compared to the multi-varied reality of the internet where information is copied endlessly.

Is fragmentation of the internet a threat?

Various authors mention the balkanisation or fragmentation of the internet, where the internet would be separated into regional fractions, as a threat to the internet. A fragmented internet has connotations such as an ‘EU cloud’, a ‘BRICS Internet’ or a ‘halal internet’. Examples of fragmentation vary from restrictions under national law leading to the blocking of websites containing child pornography (in many jurisdictions) and licensing agreements containing regional limitations in the sphere of broadcasting of content over the internet to specific jurisdictions blocking larger parts of the internet. Fragmentation would thus enable certain governments to censor communication.

The Pew Research Center reports as one of the major threats to the internet that “Actions by nation-states to maintain security and political control will lead to more blocking, filtering,

---

428 E.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet Policy and Governance – Europe’s role in shaping the future of Internet Governance, COM/2014/072 final.
429 Chapter 2, Section 4 of this study.
430 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
431 This study uses the term ‘fragmentation’ and its derivatives as alternatives for the term ‘balkanisation’: see Morgus and Maurer in their blogpost of 19 February 2014, available on: http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html.
segmentation, and fragmentation of the Internet.” This is a threat from the point of view that one of the main achievements of the internet is creating a global platform for communication, exactly because one of its main features is the absence of borders. The European Commission also supports the point of view that the internet should be one unfragmented space. There are different rationales behind this point of view, but an essential element is in any event a global view on the freedom of speech or communication: internet users can send information to and receive information from the whole world.

Also Chander & Lê warn that measures by governments all over the world are creating barriers to the free flow of information across the globe, as a result of which the very nature of the World Wide Web is at stake. In a paper on what they call ‘data nationalism’ they give a – wide-ranging – overview of a variety of measures of national governments and the European Union and of the rationales behind these measures. Chander & Lê discuss the framework for transfer of personal data under Directive 95/46 on data protection as a barrier to the free flow of information. They also mention proposals to build an infrastructure where data remain confined within limited jurisdictions, like the EU cloud or a BRICS Internet, as a reaction against foreign surveillance, mainly by the United States. They give different rationales for measures of national governments: protecting nationals against foreign surveillance, enhancing privacy and security (for other reasons), supporting domestic law enforcement by keeping data within a jurisdiction, supporting the domestic economic development by protectionist measures hampering the free flow of information, and finally what could be summarised as censorship.

Various authors argue that fragmentation would adversely affect privacy and security on the internet. The consequences for privacy and security could be negative where considerations of national sovereignty (leading to censorship) and economic advantage motivate fragmentation and where fragmentation links to monitoring of internet users. However, from the perspective of privacy and data protection, fragmentation is not necessarily a disadvantage. One of the suggestions to better protect EU citizens against

---

436 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet Policy and Governance – Europe’s role in shaping the future of Internet Governance, COM/2014/072 final, at 1.
438 Under Article 25 of Directive 95/46 transfer of personal data outside the EU requires an adequate level of protection in the country of destination. See Chapter 9 of this study.
439 E.g., Cloud for Europe, a project co-funded by the European Commission under the Framework Programme for Research and Innovation (FP7), see: http://www.cloudforeurope.eu/. Chander and Lê mention that the idea of keeping data in Europe was proposed by the German Chancellor Merkel.
440 This study does not follow the order of the paper, but puts it in an order which is more logical in the study’s specific perspective.
442 Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson and Orla Lynskey, “Internet Balkanization gathers pace: is privacy the real driver?”, International Data Privacy Law, 2015, Vol. 5, No. 1.
foreign surveillance is the development of an EU cloud, where personal data remain confined within the EU territory. This suggestion is aimed at guaranteeing that the European Union has jurisdiction to ensure protection and that the personal data of individuals in the Union cannot be accessed by authorities of third countries.

The picture is not clear. Considerations of privacy and data protection could justify measures that might result in fragmentation, but it should also be taken into account that privacy and data are essential values for a democratic society. Considerations of privacy and data protection do not justify acts of governments that adversely affect the democracy on the internet. A debate between the CNIL, the French DPA, and representatives of Google following the implementation of Google Spain and Google Inc. demonstrates the complexity. The CNIL ordered Google to apply the delisting of certain searches based on names of individuals on all domain names of the search engine, including google.com. The Google Privacy Council reacted in a blog by explaining that this order would set the precedent for other regimes limiting the democratic freedoms on the internet, criminalising speech critical of their leaders or speech qualified as gay propaganda.

5. The Internet in terms of Freedom and Powers: Is there a Shift from Freedom to Power?

Freedom, a free internet as a common good

A further dimension of the information society is freedom, the notion that a free internet is a common good, of course provided that fundamental rights of privacy and data protection are respected.

Freedom in the context of the internet has various connotations. In one sense, freedom relates to economic freedoms, considering that the internet is a trigger for economic growth based on a free flow of information. In another sense, freedom relates to the possibility to enjoy freedom of expression and other human rights through the internet, which also fosters democratic participation. This connotation also includes the absence of censorship. Proponents of the internet also consider the absence of government intervention as such as a great improvement enabled by the internet. This is a reason why the ICANN model with a

---

443 E.g., Cloud for Europe, see footnote 439.
444 See Chapter 2 of this study.
multi-stakeholder process receives wide support, also from the European Commission.\textsuperscript{450} Finally, freedom also means that the internet is a (global) public space where persons are free,\textsuperscript{451} a freedom that would be prejudiced if the internet were fragmented.

The United Nations High Commissioner for Human Rights describes the added value of the internet for our societies and for individuals foremost in terms of freedom, for reasons closely connected to the advantages of networked societies and globalisation. He sees the internet as boosting freedom of expression.\textsuperscript{452} The internet is supposed to protect human rights and foster innovation, creativity, and economic growth.\textsuperscript{453}

The relation between internet freedom and net neutrality (or network neutrality) is often made. Commentators consider net neutrality as being more than an economic principle.\textsuperscript{454} Net neutrality must ensure that the internet does not favour one application or service over another. In his paper from 2003,\textsuperscript{455} Wu coins the term and makes the case for net neutrality, which he ultimately understands – together with an internet that is open and accessible for everyone – as the concrete expression of belief in innovation. Freedom can also mean the freedom to switch between networks and not be constrained to a specific network.\textsuperscript{456} More generally, net neutrality is considered to be a key instrument in support of the protection of fundamental rights on the internet, in particular the freedom of expression. In this view, privacy and data protection also benefit from net neutrality, since these fundamental rights prohibit discriminatory treatment of communications that sometimes require the monitoring of personal information.\textsuperscript{457}

\textsuperscript{450} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet Policy and Governance – Europe’s role in shaping the future of Internet Governance, COM/2014/072 final, at 5.

\textsuperscript{451} P. Bernal, Internet Privacy Rights, Rights to Protect Autonomy, (Cambridge University Press, 2014).


\textsuperscript{456} This is obviously linked to a market with free competition. Also, this connotation is reflected in the idea of data portability, in Article 18 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.

\textsuperscript{457} Andrew McDiarmid and Matthew Shears, “The Importance of Internet Neutrality to Protecting Human Rights online”, in: Luca Belli and Primavera De Filippi (eds), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, available on: https://hal.archives-ouvertes.fr/hal-01026096, at 28-31.
Commentators argue that this free internet is under threat. Benkler describes the shifts of powers and freedoms as a consequence of the very existence of the internet, substantially changing the powers and freedoms in our societies.\footnote{Yochai Benkler, “Networks of Power, Degrees of Freedom”, International Journal of Communication 5 (2011), pp. 721-755, Harvard Law School.} To put it shortly, whereas the internet, in its initial stage, shifted power to and created more freedom for the individual, there is now a tendency that freedoms are becoming more limited with powers being retrieved by governments and powers also shifting towards big companies. Greenwald mentions the turn of the internet from representing an extraordinary potential for democracy to becoming a tool for government repression.\footnote{Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State (Metropolitan Books/Henry Holt (NY) 2014), at 6.}

Governments may take back powers for reasons of national security or law enforcement, by accessing and using large amounts of information on the internet for these purposes, or even to impose censorship on the internet, which is a practice in several countries with a lower level of respect of western democratic values.\footnote{The case of censorship in China and Russia is elaborated in Dutch in: Adviesraad Internationale Vraagstukken (AIV), Advies 92, Het Internet: een wereldwijde vrije ruimte met begrensde staatsmacht, November 2014, at 62-63.} These practices pose threats to internet freedom and the open structure of the internet and possibly lead to geographical fragmentation, as was explained above. There is a risk that trust in a free internet will evaporate as a result of revelations about government and corporate surveillance. There exists also a risk that this surveillance will further increase.\footnote{Janna Anderson and Lee Rainee, “Net Threats, Experts say liberty online is challenged by nation-state crackdowns, surveillance, and pressures of commercialization of the Internet”, Pew Research Center, available on: http://www.pewinternet.org/2014/07/03/net-threats/}

\textit{Power on the internet}

Power as a dimension of the information society obviously has a bearing on freedom. Benkler describes power as the capacity of one entity to alter the behaviour, outcomes, or configurations of others, whereas freedom relates to influencing one’s own behaviour.\footnote{Yochai Benkler, “Networks of Power, Degrees of Freedom”, International Journal of Communication 5 (2011), pp. 721-755, Harvard Law School.}

Power in networked societies is a complex concept, as Castells explains.\footnote{Manuel Castells, “A Network Theory of Power”, International Journal of Communication 5 (2011), pp. 773-787, 1932-8036/20110773. This paper is worth reading, because it identifies different forms of power and counter power.} Power is exercised on various levels and is not one-dimensional. For example, in global capitalism the global financial market has the last word, whereas in the political arena it is the government of the United States that holds a strong military position. Castells mentions that this military power could not prevent the financial crisis.\footnote{Manuel Castells, “A Network Theory of Power”, International Journal of Communication 5 (2011), pp. 773-787, 1932-8036/20110773, at 775.} In networked societies power is exercised through inclusion and exclusion in networks, setting of standards, the domination of social actors over other social actors, and the relations between networks following the strategic
alliances between the dominant actors.\textsuperscript{465} Where there is power, there is counterpower in a networked society, resisting established domination.\textsuperscript{466}

In addition, on the internet a shift of power is taking place towards big internet companies and to governments for reasons of national security and law enforcement. At least, this is the perception articulated by Benkler and Greenwald. The power relations’ complexity also means that there may be a power vacuum on the internet. The shift of power referred to does not only challenge the freedom of internet users in a global, networked society, it also leads to – the perception of – loss of control of the European Union and of national governments exercising their mandates in the area of privacy and data protection, be it through the judiciary, the legislator or supervisory authorities. As a result, individuals also lose control over their personal data.

It is against the backdrop of this reality that we discuss the mandate of the European Union under Article 16 TFEU on privacy and data protection. Where big companies and governments exercise power on the internet, this requires a counterpower to protect the rights and freedoms of individuals. This counterpower must ensure that individuals can effectively exercise their rights and freedoms. Empowerment of individuals – by improving individuals’ ability to control their data – is an objective of the data protection reform.\textsuperscript{467}

This study identifies six phenomena that present a challenge to the mandate of the EU on privacy and data protection under Article 16 TFEU in the information society which is meant to ensure that individuals can effectively exercise their rights and freedoms. These phenomena may adversely affect the role of counterpower in an information society. These phenomena are presented as an introduction to the two central themes of this chapter: the era of big data where our economies are largely data driven and (mass) surveillance by private companies and governments. The phenomena are an illustration of the complexity and do not intend to give an exhaustive overview of the reality on the internet.\textsuperscript{468}

First, uncertainty. New technologies and IT applications are developed and deployed at a continuously high pace. The resulting technological turbulence\textsuperscript{469} leads to uncertainty. The quote of Castells at the start of Section 2, explaining that we live in confusing times is a confirmation of this uncertainty.

\textsuperscript{468} A similar, but not equal list is found in: Lee A. Bygrave, Data Privacy Law, An International Perspective (Oxford: Oxford University Press, 2014), at 9.
Second, lack of transparency. The lack of transparency on the internet relates to the behaviour of big internet companies and also of governments, for instance where governments are processing information for law enforcement or national security purposes. Prins argues that governments themselves develop and use IT applications on a de facto basis without awareness of the larger whole.\textsuperscript{470} This lack of awareness implies a lack of control and also leads to insufficient accountability of governments.

Third, security threats. The internet is vulnerable, because of flaws in cybersecurity. These flaws may be the result of any form of cybercrime or of unintentional security breaches. We refer to the special issue of The Economist,\textsuperscript{471} discussed before.

Fourth, increased visibility. Individuals are increasingly visible, which reduces the privacy individuals enjoy and may make them a target for wide monitoring, resulting in profiling. Reidenberg qualifies this increased visibility as a privacy turning point, mainly in relation to the state. He mentions for instance the reversal of the presumption of innocence.\textsuperscript{472} One could argue that a similar turning point may be reached in relation to the big internet companies.

Fifth, automated decision-making. When decision-making is automated, it becomes less understandable and predictable, increasing the possibility of misuse of data, or possibly even a dehumanisation of societal processes.\textsuperscript{473} The challenge we face relates to the ‘datafication’\textsuperscript{474} of societies, as explained below in the context of big data. More generally, technology allows permanent monitoring of online behaviour for unstated purposes.\textsuperscript{475}

Sixth, asymmetric market structure. The market structure in the information economy is asymmetric, with a few overwhelmingly dominant players and more generally, an imbalance between big companies on the one side, and SMEs and individual users on the other side.\textsuperscript{476} Information has become an asset. The economy is driven by information and in two-sided business models personal data have become a currency for individuals to pay for services.\textsuperscript{477}

\textsuperscript{471} Economist, A special report on cyber-security, Defending the digital frontier, 12 July 2014. See Section 4 of this chapter.
\textsuperscript{472} Joel Reidenberg, “The Data Surveillance State in the United States and Europe”, Princeton University - Center for Information Technology Policy; Fordham University School of Law, November 2, 2013, Wake Forest Law Review, Fordham Law Legal Studies Research Paper No. 2349269, at 3.
\textsuperscript{473} As explained by Lee A. Bygrave in Data Privacy Law, An International Perspective (Oxford: Oxford University Press, 2014).
\textsuperscript{476} It is recognised as a major risk for the internet that commercial pressures affecting everything from internet architecture to the flow of information will endanger the open structure of online life; see: Janna Anderson and Lee Rainee, “Net Threats, Experts say liberty online is challenged by nation-state crackdowns, surveillance, and pressures of commercialization of the Internet”, Pew Research Center, available on: http://www.pewinternet.org/2014/07/03/net-threats/.
\textsuperscript{477} European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on “Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”, notably at 10-13.
The concept of net neutrality may not only lead to a low barrier to internet entrance for start-up companies or for individuals wanting to share information, but it also has as an adverse effect that it works to the advantage of the big players on the internet.\textsuperscript{478} This all leads to a shift of control to these internet companies.

6. **Big Data justifies a Qualitative Shift in Thinking**

The evolving era of big data implies, by its very nature, a lack of control, since the volume of data is unprecedented, diverse in variety and moving with a velocity that is increasingly approaching real time.\textsuperscript{479} The availability of massive amounts of information has also allowed governments to use this data as source for mass surveillance. Control decreases by what Mayer-Schönberger & Cukier call ‘datafication’,\textsuperscript{480} which refers to the self-evident relation between data and people without the individuals concerned being able to control the accuracy of the information.\textsuperscript{481} Big datasets can be used for real-tracking and predictive analysis.\textsuperscript{482} This perceived lack of control is also the consequence of the ease of data distribution and data searches, combined with the difficulty of data deletion.\textsuperscript{483}

Having said this, big data and analytics on the basis of big data create benefits for individuals and society. For governments big data can be the basis for exponential improvements in policy-making. A telling example is health care where on the basis of large amounts of health records diseases can be detected and treated. Since not all patients are alike and individuals react differently to treatment, the use of vast amounts of data makes personalised treatment possible. Mobile devices connected to large datasets could help the detection of symptoms of illnesses. Health care is just one out of a large number of examples mentioned in the PCAST Report written for President Obama.\textsuperscript{484}

There are many definitions of big data, and there is also disagreement as to whether this phenomenon is really new and fundamental to our society. This disagreement is linked to the question whether big data really justifies a qualitative shift in thinking about the collection and use of information in an information society.

**Big data is really new and a fundamental change**

\textsuperscript{478} Because of requirements on Quality of Service, see European Parliament, Directorate-General for Internal Policies, Policy Department A, Economic and Scientific Policy, Network Neutrality Revisited: Challenges and Responses in the EU and in the US, December 2014, at 24 and 101-102.

\textsuperscript{479} The three V’s; see: “Big Data: Seizing Opportunities, Preserving Values”, Executive Office of the President (Podesta Report), at 4.


\textsuperscript{481} Although data subjects have the right of rectification of non-accurate personal data, under Article 8(2) Charter.

\textsuperscript{482} José Van Dijck, Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society 12(2), 2014: 197-208, at 199.

\textsuperscript{483} Three characteristics mentioned in: Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing, 2013, at 46.

\textsuperscript{484} Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology, (PCAST Report) May 2014, Section 2.
This study takes the view that big data is a development too important to ignore in considering the issue of privacy and data protection on the internet. This is in line with the views of Kohnstamm who explains that big data puts our society at risk: “Full individual development will become an illusion when too many choices are made for you on the basis of a profile. […]. Personal freedom shouldn’t be defined by what businesses and governments know about you.”

Valuable sources that claim big data is really a new phenomenon and represents a fundamental change are the two reports written for President Obama in May 2014, known as the Podesta Report and the previously mentioned PCAST Report. The Podesta Report states that “data is now available faster, has greater coverage and scope, and includes new types of observations and measurements that previously were not available.” The Podesta Report refers to this development as the ‘3 Vs’: Volume, Variety and Velocity. The cost of data collection has declined, leading to an explosion of data, combined from a variety of sources (email, web browsing or GPS locations are just a few examples). As the report states, the processing of data takes place with a velocity approaching real time.

Another fundamental change relates to the value of what is called ‘metadata’, a notion stemming from telecommunications that played a role in the surveillance by the NSA and also in the ruling of the Court of Justice in Digital Rights Ireland and Seitlinger. Metadata relates to the called and calling phone numbers, to the time and the place where a conversation takes place and excludes the content of a conversation. Metadata have always been considered as being less revealing than content data. In the era of big data this paradigm changes, as Schneier explains. The combination of sets of metadata becomes more revealing than the content of a conversation itself. Schneier states: “Eavesdropping gets you the conversation; surveillance gets you everything else.”

---

485 Quote taken from Annika Sponselee, “Privacy with a View – Part II”, Privacy & Practice 01-02/2015, at 71-78.
489 Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (Podesta Report), at 4-5.
490 Section 215 of the US Patriot Act 2001 only relates to metadata. The US government emphasised that the NSA only collected metadata; see: Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015), at 20.
491 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
493 Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (Podesta Report), at 34.
494 See also Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015), at 17-21.
Big data has a societal impact, because of two main *raisons d’être*: big data enables unprecedented predictions on private lives and it shifts the power to those who hold the information and those who supply it. Mayer-Schönberger & Cukier, too, mention, in their book on big data, a number of societal changes that are due to big data. In their view would require a fundamental rethinking of legislative arrangements, such as on privacy and data protection. They note that what they call the three core strategies to ensure privacy – individual notice and consent, opting out and anonymisation – lose much of their efficiency.

In the EU context there is a further consequence: purpose limitation is a substantive principle of EU data protection law, included in Article 8 Charter, which means, in essence, that collection of data should take place for a specific purpose. The principle of data minimisation as laid down in Article 6(1)(c) of Directive 95/46 on data protection is related to this. In a big data context, personal data collection takes place for unspecified purposes and on a massive scale. An exponent of a school of thought pleading for modification of the substantive principles of data protection is Nissenbaum. She pleads for replacing principles like data minimisation and purpose limitation by new concepts based on the context of data processing activities. Such fundamental changes to the substantive principles are difficult to reconcile with EU data protection law.

In their book, Mayer-Schönberger & Cukier explain the substantive changes resulting from analytics based on correlations between data, instead of causality. Organisations do not only base future propensities of behaviour on individuals’ past behaviour, but they also seek to predict the future on the basis of non-intuitive statistical correlations. This method can enhance the quality of decision-making in an unprecedented way to the benefit of society, so they say. They start their book with a telling example, by explaining how the spread of a flu virus could be stopped, with the help of big data use, based on Google search terms. The search terms used by internet users enabled areas infected by the flu virus to be identified.

---

498 Helen Nissenbaum, Privacy in context (Stanford University Press, 2010). Challenging her proposals falls outside the scope of this study.
499 Ja____^\text{\textsuperscript{499}}\text{\textsuperscript{499}}\text{\textsuperscript{499}}}ames Rule, Douglas McAdam, Linda Stearns and David Uglow, The Politics of Privacy, Planning for Personal Data Systems as Powerful Technologies (Elsevier, 1980), at 133.
500 Other interesting examples can be found in: Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology, (PCAST Report), Chapter 2.
messy. This does not sit well with the right of rectification of non-accurate personal data, a right of the data subject under Article 8(2) Charter.

**Big data is pervasive in the daily life of individuals**

Big data is closely connected to the Internet of Things, described as “a future in which everyday objects such as phones, cars, household appliances, clothes and even food are wirelessly connected to the Internet through smart chips, and can collect and share data.” This makes the use of information even more pervasive in the daily life of individuals, as an example in the Podesta Report illustrates: signals from WiFi networks at home reveal the people in the room and where they are seated, and power consumption may show people moving around a house. The Podesta Report is an interesting starting point for a short reflection on some novel developments.

In earlier years, the collection of large amounts of personal data sparked off debates on proportionality under data protection law, partly because large scale collection was not considered an effective means in combating crime. The collection of those data could be seen as disproportional, because it lacked effectiveness. We quote one of the essentials of the Information Management Strategy for EU internal security: “a well targeted data collection, both to protect fundamental rights of citizens and to avoid an information overflow for the competent authorities”. The targeted collection was based on the adage ‘select before you collect’, to avoid that one has to find the needle in the haystack.

However, big data changes the paradigm. One can collect large amounts of data and draw effect from it. In other words: one can find the needle in the haystack. The Podesta Report underscores that finding a needle in a haystack is not only possible but also practical: in order to find the needle you have to have a haystack.

Perfect personalisation becomes possible and can create a clear picture of an individual. This may be useful in a consumer context, leading to personalised offers of goods and services, but also entails risks of discrimination or exclusion of persons, or even worse of suspicions of persons, not based on facts, but on predictions.

---


503 Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (Podesta Report), at 53.

504 See, in particular, pp. 5-9 of the report. The report also mentions the persistance of data, a subject that is also relevant in relation to the right to be forgotten, and the ruling in Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.


506 This is also what former NSA Director Alexander said; see: Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015), at 138.

507 This is closely related to targeted and behavioural advertising, which is not always perceived as positive from the perspective of privacy and data protection.
Anonymisation of information is considered an effective means of addressing privacy concerns. In terms of data protection, if data are anonymised they no longer fall within the definition of personal data\textsuperscript{508} and the EU legal framework is no longer applicable. However, the effect of anonymisation is diminishing. Integrating various data without personal identifiers may lead to re-identification. The Podesta Report touches upon the uncertainty as to how under these circumstances the individual can retain control.

Big data is also a driver behind the discussion on the nexus between privacy and competition, based on the assumption that (big) data are an asset in the information society, and facilitate the ‘two-sided’ business model, where individuals pay for ‘free’ internet services by handing over personal data\textsuperscript{509}. The acquisition of personal data is a key success factor for online service providers.\textsuperscript{510} Jones Harbour expects “businesses generating both more detailed and more holistic profiles of their users than ever before”.\textsuperscript{511}

7. People can no longer evade Surveillance through Electronic Means

Surveillance – as an instrument of government – is related to the political climate and to actual or perceived threats to public security, and plays its part in the relations between the EU and the US on security related issues.\textsuperscript{512} Over the last number of years, technological development has enabled surveillance to become widespread in various areas of government intervention, monitoring wide categories of data. Many of the debates on surveillance, provoked by the Snowden revelations and – in the European Union – by the now annulled Directive 2006/24 on data retention,\textsuperscript{513} stem from the particular problem of the surveillance of communications data. Surveillance applies to wide categories of data. An example outside the area of communications is financial data, the subject of the Agreement between the European Union and the United States on the processing and transfer of financial messaging data from the EU to the US for the purposes of the Terrorist Finance Tracking Program.\textsuperscript{514} We also refer to passenger data, the subject of a number of instruments for Passenger Name

\textsuperscript{509} The subject of: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”.
\textsuperscript{512} These topics play a role in various other chapters of this study.
\textsuperscript{513} Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
Records (PNR), and hotels records, the object of a case before the US Supreme Court. These hotel records may be sensitive, where they may reveal that a person participated in meetings of political parties or of groups of activists taking place in or around a hotel.

In itself surveillance is nothing new in the context of developing technologies. In 1967 Westin wrote already on various forms of surveillance (physical surveillance, psychological surveillance and data surveillance) that may impact on the privacy of individuals. More recently, a report on the surveillance society (2006), commissioned by the Information Commissioner of the United Kingdom starts as follows: “We live in an information society. It is pointless to talk about surveillance society in the future tense.” The large-scale surveillance that came to the surface following the Snowden revelations confirmed – to use an understatement – this point of view.

It is difficult to imagine an information society where surveillance is absent. This study focuses therefore not on surveillance as such, but on the extent to which configurations of surveillance are in conformity with constitutional values. This requires an analysis based on an understanding of the various aspects of surveillance.

**Surveillance from different perspectives**

One perspective for looking at surveillance is to regard it as a product of new technologies that has an intrusive impact on the freedom of the individual. This perspective has been the most predominant in the public debate, be it on mass surveillance by governments for security purposes or on the use of personal data by search engines or social media providers. It is also a key element in this study on privacy and data protection on the internet.

In his book *No place to hide*, Greenwald explains the impact of government surveillance on the internet in an illustrative way. The genuine new dimension of this type of surveillance may not be its massive scale, but the role now played by the internet is in our daily lives. People can no longer evade surveillance and surveillance extends to virtually all forms of human interaction. This is especially problematic, since the internet is supposed to be a place where individuals should be able to express themselves anonymously, make mistakes and

---

519 See also Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015).
520 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State, in particular at 5-6, 46, and 174–180, also referring to research relating to Watergate.
521 Although the massive scale is important. Greenwald refers to the ‘collect it all’ philosophy of the NSA, at 95, 169 of his book.
522 This is a statement of Greenwald, but a nuance will be given below.
explore their identities. Surveillance may have a chilling effect on the freedom of expression.523

Surveillance can also be seen from a different perspective, as “the outcome of bureaucracy and the desire for efficiency, speed, control and coordination”.524 As explained by Mayer-Schönberger & Cukier, tools of surveillance, based on big data may significantly improve the quality of public policies and services.525

The purposes of surveillance should be taken into account when assessing the adverse effects on the privacy of the individual. Governments – but, in certain circumstances also private actors – should base their acts on a balancing of the various interests at stake.526 A proper balancing means that privacy should not be outweighed by other interests, justifying surveillance. An example of a society that no longer values privacy can be found in the novel The Circle by Dave Eggers.527 This novel describes a company whose philosophy is that secrets are lies and privacy is theft.528 The surveillance within this company was at such a level that the protagonist had to justify herself for escaping surveillance by her employer during a few hours on a Sunday afternoon. Schmidt & Cohen describe a similar scenario, in a different context. They refer to individuals wanting to have nothing to do with profiles, data systems or smartphones. Governments may suspect that people who opt out completely from technology have something to hide and may consequently wish to include them in a hidden people registry.529

Currently, surveillance is facilitated by the fact that individuals disclose information on a voluntary basis online. Sometimes, people can evade surveillance. In the near future this may no longer be the case. Developments relating, for instance, to drones or facial recognition will magnify the intrusiveness of surveillance for privacy and data protection. Privacy and data protection become even more important.

**Different types of surveillance, but the distinctions are not always crystal clear**

Different categories of surveillance on the internet can be distinguished, although these distinctions are not always crystal clear and not all categories are equally relevant. The first distinction is between surveillance by states and surveillance by private companies. The second distinction regards mass surveillance and targeted surveillance. A further distinction, relevant for surveillance by states, is the distinction between internal and foreign surveillance.

523 See also Bruce Schneier, Data and Goliath, (W.W. Norton & Company, 2015), at 95-98.
525 Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (Eamon Dolan/Houghton Mifflin Harcourt, 2013), e.g. the example in 3.2 thereof on the prediction of the spread of flu.
526 Chapter 5 will further explore the legal aspects of this balancing.
527 Dave Eggers, The Circle (McSweeney’s, 2013).
528 See in this context also the statement of Zuckerberg that privacy is no longer the norm, mentioned in Chapter 2, Section 3 of this study.
Mass surveillance by the state – more particularly by a US intelligence agency, the NSA, as revealed by Snowden – was a main trigger for this study. The best known programme under which this surveillance allegedly took place was PRISM, which gave the NSA direct access to the central servers of leading internet companies based in the US and allowed the collection of various types of personal data. The collection of personal data by US intelligence agencies was based on Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) and Section 215 of the USA Patriot Act 2001.534

These two legal bases are mentioned here, because they also underline the distinction between internal and foreign surveillance.535 Sometimes – not only in the US – a state has powers for foreign surveillance, outside its national borders, which are wider and subject to less safeguards for individuals than the powers for surveillance of individuals within its territory. Section 702 FISA relating to foreign surveillance included the monitoring of the content of communications and also permitted what is called ‘upstream collection’, the interception of internet communications by the NSA. Section 215 Patriot Act was limited to ‘metadata’, thus excluding content, and the use of this power is subject to stricter oversight.

Mass surveillance by the state is also a phenomenon within the European Union. The Snowden revelations referred to activities of GCHQ, an intelligence agency of the United Kingdom, and also other Member States are engaged in large scale surveillance activities. Moreover, mass surveillance is not necessarily limited to intelligence agencies and national security. An example is the Automated Number Plate Recognition, used as an instrument for the enforcement of traffic law.540

530 Planning Tool for Resource Integration, Synchronisation and Management (PRISM) of the NSA.
534 This act also amended FISA, 50 U.S.C. 1861.
536 E.g., interception on internet cables. Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013. Please note that this interception falls outside PRISM.
539 European Parliament, Directorate-General for Internal Policies, Policy Department C, Citizens’ Rights and Constitutional Affairs, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law. This report mentions Sweden, France, Germany and the Netherlands as countries engaged in large-scale interception and processing of communications data.
540 For instance, used for average speed cameras (trajectcontrole) which are in place in the Netherlands and some other European countries. Source Wikipedia, Dutch page on trajectcontrole.
The opposite to mass surveillance is targeted surveillance. Targeted surveillance is not directed at large groups of the population but at specific individuals, for instance those suspected of or otherwise connected to terrorism or other serious crime. Possibly, targeted surveillance also extends to their networks.

However, the distinction between mass surveillance and targeted surveillance is not clear, of which the obligations under the Directive 2006/24 on data retention, which was annulled in Digital Rights Ireland and Seitlinger,541 provide a telling example. The data involved were collected and retained on a massive scale, but law enforcement authorities were only permitted to use them for specific, targeted purposes. This situation could qualify as targeted surveillance on the basis of the reasoning that targeted surveillance might include targeted use, on the basis of specific warrants, of massively collected metadata.542 In the reasoning of the European Court of Justice the obligations under Directive 2006/24 seemed to qualify as massive surveillance,543 since the Court considered that whole parts of the population could have the feeling of being under constant surveillance. Blurry as it may appear, the distinction remains important. As stated in a study for the European Parliament: “It is precisely the purposes and the scale of surveillance that differentiates democratic regimes from police states.”544 It is the massive scale of surveillance that leads to the most serious breaches of fundamental rights.545

Mass surveillance by private companies for their own commercial purposes is closely related to big data, especially where surveillance takes place as part of core business activities. Exponents are the ‘two-sided’ business model of search engines and social media platforms where individuals pay for the services they receive by handing over personal data.546 Other exponents are emerging services like data brokers,547 companies that collect and resell large amounts of personal data for a variety of purposes. Surveillance by companies in connection to security or to detect fraud has a different nature: targeted surveillance is normally sufficient.

541 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
543 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 37.
546 European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on “Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”, Section 2.
8. No Strict Distinction between Surveillance by the State and by the Private Sector

Private companies play a role in government surveillance. Companies are regularly required to assist law enforcement, because private companies – not governments – are in possession of the information that facilitates police work.

This cooperation between the private and the public sector was an important topic in connection with the Snowden revelations and PRISM, in what can be described as front-door and backdoor access\(^\text{548}\) by national authorities to personal data of private companies, such as cloud providers. The increasing role of private companies assisting in law enforcement leads more in general to a blurring of the dividing line between the public and private sector. As explained, PRISM allowed the NSA to gain direct access to the personal data stored in databases of the big US-based internet companies.\(^\text{549}\) Although the Snowden revelations – as far as they relate to PRISM – made this development most visible, this obviously is an issue that is not confined to the United States. A recent example within the European Union is the Proposal for a Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.\(^\text{550}\) This proposal provides for the transfer by air carriers of passenger name records to authorities of the Member States.\(^\text{551}\)

In the US, the need for cooperation of the private sector in law enforcement – and in particular the availability of information in the hands of private actors – is acknowledged in quite a number of sectoral federal privacy laws. These laws allow access by government, but at the same time they contain restrictions to this access, for instance by requiring a subpoena or a warrant, and by requiring advance notice to the individual.\(^\text{552}\) Examples are the Electronic Communications Privacy Act\(^\text{553}\) and the Stored Communications Act.\(^\text{554}\) The cooperation of the private sector in law enforcement – although well defined in statutory law – is said to be difficult to reconcile with the protection given under the US Bill of Rights as this Bill grants individuals protection against acts of the government, not against acts of the private sector.\(^\text{555}\)


\(^{549}\) Further read: European Parliament, Directorate-General for Internal Policies, Policy Department C, Citizens’ Rights and Constitutional Affairs, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law.


\(^{551}\) Article 1 of the proposal. The negotiations within the European Parliament took very long, precisely because of the privacy intrusiveness.


\(^{553}\) 18 U.S.C. § 2510.

\(^{554}\) 18 U.S.C. § 2703.

\(^{555}\) As will be explained in Chapter 6, Section 12 of this study.
Besides blurring the responsibilities of the state and the private sector, where the latter assists in law enforcement or national security, this cooperation with the private sector also raises jurisdictional issues, since surveillance in the cloud is partly transnational. Furthermore, public-private cooperation may lead to countermeasures of affected states, aiming at securing their databases from access by foreign countries. The EU cloud, mentioned before, is an example.\textsuperscript{556} This in turn may have an impact on the global structure of the internet.\textsuperscript{557}

Another topic mentioned in relation to transnational surveillance is the potential impact on fair competition. A report written for the European Parliament contains the allegation that the secrecy of surveillance by a state in close cooperation with private companies based in that state implies that the surveillance covers economic intelligence.\textsuperscript{558}

\textit{The various types of surveillance are not necessarily different in terms of intrusiveness}

The distinctions between the various types of surveillance are relevant for the degree of intrusiveness of surveillance on the privacy of individuals. Mass surveillance is a main source of threat to privacy, because of its scale and also because of the normally secret nature of surveillance measures. There is abundant case law of the European Court of Human Rights on secret surveillance, confirming that mass surveillance is one of the main threats to privacy.\textsuperscript{559} Secret and massive surveillance has an impact on our democratic societies, since collective freedom is a common good and transparency of government is a requirement for a functioning democracy. Secret and mass surveillance also has an impact on individuals, since its chilling effect may lead to adaptation of behaviour, moving away from non-mainstream behaviour, as explained by Greenwald.\textsuperscript{560}

These considerations do not imply that targeted surveillance is necessarily less intrusive and hence more in conformity with the principle of proportionality as developed in the case law on fundamental rights. Targeted surveillance may be based on discriminatory criteria and the result may be stigmatisation, for instance where specific groups in our society are the targets of intensive targeted surveillance.\textsuperscript{561} This is a topical theme, after the attacks on Charlie

\textsuperscript{556} See Section 4.
\textsuperscript{558} European Parliament, Directorate-General for Internal Policies, Policy Department C, Citizens’ Rights and Constitutional Affairs, National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, 2013, at 8. The paper does not provide evidence.
\textsuperscript{560} See Chapter 2, Section 3 of this study.
\textsuperscript{561} A parallel could be drawn with \textit{S. and Marper v UK}, Applications Nos. 30562/04 and 30566/04, 4 December 2008. In that case before the ECtHR the element of stigmatisation played a role, where the applicants in the case where included in a targeted (albeit huge, but that is not relevant here) DNA database.
Hebdo in January 2015 and the wider problems of foreign fighters leaving their home countries to take part in armed conflicts abroad.\textsuperscript{562}

Surveillance by government is not by definition more intrusive than surveillance by private actors. The following example relating to Directive 2006/24 on data retention\textsuperscript{563} and the German implementing law illustrates this. For the German Constitutional Court, it was a factor in favour of the compatibility of the directive with the German Constitution that traffic data were not stored by the state, but by private companies.\textsuperscript{564} The European Court of Justice however – without explicitly taking the opposite view – mainly highlighted the disadvantages of storage by private companies: the fact that these companies were able to take economic considerations into account when deciding on the level of security and could decide to store the data outside the European Union would complicate the control.\textsuperscript{565} This example relates to a situation where storage by private actors takes place in the context of government activities. However, surveillance by private companies for commercial purposes may also be particularly intrusive, for instance where sensitive information is included, such as tracking of individuals in connection with financial or health related services.

*Democratic legitimacy and accountability of surveillance, in relation to secrecy and cooperation with the private sector*

Surveillance also raises a number of questions in relation to democratic legitimacy and accountability. Often secrecy is an element of surveillance. Secrecy may to a certain extent be justified to avoid that the person under surveillance frustrates the results of surveillance. However, secrecy also complicates the democratic legitimacy of governmental actors, as it does judicial control under the rule of law. This is the case in particular where national security is involved and secrecy prevents authorities from being accountable for their acts. Limitations in the oversight on surveillance – by the judiciary or by the legislative branch of government – challenge the legitimacy of surveillance activities themselves.

From the perspective of democratic legitimacy and accountability it is not evident that companies assist in government surveillance. The cooperation with private companies blurs the responsibilities, is difficult to reconcile with the state monopoly on law enforcement and connected to this monopoly with the need for full accountability of state action.

Cooperation with private parties in government surveillance may also result in a situation where the constitutional guarantees surrounding law enforcement are insufficiently guaranteed. In our democratic societies police and judicial authorities are subject to strict

\textsuperscript{562} See: Foreign Fighters under International Law, Academia Briefing No 7, Geneva Academy of International Humanitarian Law and Human Rights, October 2014.


\textsuperscript{564} Bundesverfassungsgericht Germany, ruling of 2 March 2010 in joined cases 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 on data retention, press release No. 11/2010 of 2 March 2010, at 3.

\textsuperscript{565} Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 67 and 68. Paragraph 68 will be discussed further in Chapter 7.
rules limiting their powers and ensuring the fair treatment of citizens; they are subject to scrutiny by courts which includes a right to fair trial as guaranteed by Article 47 Charter and Article 6 ECHR.

More generally, involvement of the private sector in surveillance activities complicates the legitimacy and accountability. This leads to a number of questions. How is the legitimacy and accountability of the private sector for surveillance ensured, in particular where multinational companies are involved? How can individuals invoke their rights, under the rule of law? To what extent can the effectiveness of surveillance play a role in the assessment of its legitimacy?\(^{566}\) Considerations of legitimacy and accountability of surveillance are closely related to the test of proportionality of interferences with fundamental rights under the rule of law, as a key element of the scrutiny by the Court of Justice of the European Union and by the European Court of Human Rights.\(^ {567}\) Arguably, the instrument of surveillance by governments may – under strict conditions – be acceptable for the fight against terrorism and serious transnational crime. This is not necessarily the case in relation to immigration, or other purposes of public policy. Furthermore, as part of the proportionality test, the Court of Justice considers whether there is an actual threat to society. The absence of a connection between a threat to public security and the retention of data was an element in the ruling of the Court in Digital Rights Ireland and Seitlinger, leading to the annulment of Directive 2006/24 on data retention.\(^ {568}\)

9. The Perspective of the EU and the Member States: What is changing?

The quote of Castells at the start of Section 2 not only confirms that we live in confusing times, it is also a valuable observation in view of the fact that the tasks of governments – the European Union in the same way as the Member States – as laid down in law, are necessarily based on the circumstances of the past. Constitutional values and fundamental rights have been developed on the basis of the idea that they are of a universal nature – at least in terms of time –, but now they have to be applied in new circumstances where societies are changing and have to grasp what is new.

What makes it even more difficult is the rapid pace of technological change. This rapid pace entails that governments, in particular in their role as legislators, are continuously lagging behind. Legislation requires careful reflection and democratic legitimation and that takes time. The legislative process on the reform of the EU data protection legislation is illustrative in this regard. The Commission adopted its proposals in January 2012,\(^ {569}\) after a few years of

---

\(^{566}\) This is the topic of output legitimacy, that plays a role in various parts of this study.

\(^{567}\) As will be explained in Chapter 5 of this study.

\(^{568}\) Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 67.

\(^{569}\) Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final; Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or
consultation of stakeholders, and only at the very end of 2015, after finalisation of this research, the EU legislator has agreed upon a final text.

This section takes the perspective of the European Union – and of the Member States – faced with developments in the features of the internet economy and in communications on the internet. The perceived loss of control, resulting from these developments is an issue, in particular for the Union and its Member States. Since the most dominant players on the internet have their main establishment outside the European Union and the Union and its Member States are left with only limited influence on data flows and internet governance, these developments complicate the mandate of the European Union and the Member States to ensure privacy and data protection under Article 16 TFEU. This section describes the impact of these developments on the EU mandate under Article 16 TFEU and on the Member States, discussing main areas where the roles are substantially affected. It is a bridge with the remainder of the study focusing on the mandate of the EU itself.

The governance of the internet and a declining role for the state

Not all challenges are specific to privacy and data protection of the internet. Globalisation, combined with social, economic and technological developments, has wider effects on the position of the nation-state. Power has become fragmented; there is a general tendency that the role of the nation is declining and that states are sharing governance with supranational organisations, as well as with private entities, in practice sometimes defined as multi-level governance. The specificity of the subject matter of this study is that it deals with an essential state function, the protection of fundamental rights of individuals. This increases the urgency of regaining control in this domain.

The EU has many similarities with a nation state in connection with the exercise of its mandate under Article 16 TFEU. This will be explained in the next chapters of this study. Here, we emphasise that what is said about the declining role of the nation state also influences the position of the EU.

The governance structure of the internet is an example of this declining role. It is difficult to align the governance structure with the different roles of the European Union and the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.

See, e.g., the explanatory memorandum of the proposed regulation.


Triggering this study, see Chapter 1, Section 1.


Multi-level governance is attaining wider acceptance, as is illustrated by, e.g., the Special Issue on the Constitutional Adulthood of Multi-Level Governance of the Maastricht Journal of European and Comparative Law, 2014, Vol. 21/2.
Member States, like the protection of fundamental rights and safeguarding the security of individuals. A specific complication is that the governance structure in itself hampers governments in ensuring the integrity of the system,\textsuperscript{576} which is a prerequisite for accomplishing other roles. Key elements of government power are shifting to the private sector.

However, perspectives change over time. The governance structure of the internet as a global infrastructure outside traditional frameworks is not necessarily absolute and/or desirable in the near future. An argument is that this governance structure was needed to allow the initial development of an information society, but that in the meantime the internet has come to a fully mature structure where governments should be able to give effect to their core tasks, such as the protection of fundamental rights of privacy and data protection. The discussion in this chapter on internet governance gives substance to this argument, although is not a plea for government intervention replacing the multi-stakeholder approach.

\textit{The reality of the internet changes privacy and data protection and the balancing with other fundamental rights and public interests}

The reality of the internet, big data and massive surveillance is difficult to reconcile with core data protection principles laid down in Article 8 Charter and Directive 95/46. Answers need to be given regarding the application of the principles of purpose limitation and data minimisation, as well as the notion of the data controller as the party in control of transfers to third countries. In reality, data are flowing over the whole world and are quite often not in control of one specific party. In addition, commentators argue that the deletion of data is an illusion.\textsuperscript{577} Another key principle in data protection is consent by the data subject as a condition of data processing, which does not reflect the reality of big data where data are used for purposes that are not known at the moment of collection of the data. In these circumstances consent cannot be informed.\textsuperscript{578}

Big data complicates in itself the protection of privacy and data protection, but it also influences the balancing with other fundamental rights and public interests, since privacy and data protection increasingly coincide with other fundamental rights and public interests. Personal data are used in many policy areas for analytic purposes to the benefit of society, as claimed in the publications on big data.\textsuperscript{579} This has an impact on privacy and data protection, in areas where this impact did not exist before, or at least to a much lesser extent. The various

\textsuperscript{576} Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De publieke kern van het internet, Naar een buitenlands internetbeleid, Amsterdam 2015.
uses of personal data with the objective of improving health care illustrate this tendency.\textsuperscript{580} Governments have to balance different, possibly conflicting, values and interests. The way these various balancing acts — where for instance privacy and data protection, freedom of expression, physical security and economic interests could all play a role — are performed is influenced by the changing reality of an information society.

An illustration is the balancing between the rights to privacy and data protection on the one hand and the demand to maximise the use of technology in response to serious threats to the security of society on the other hand, in a context where consensus on the outcome of the balancing is not a given fact. There may be pressure on limiting the rights of privacy and data protection in an internet environment, for instance where threats to the security of society are addressed,\textsuperscript{581} by extending surveillance powers. What makes it even more complicated is that the demand for maximising technology use and extending surveillance powers is highly time- and place-dependent. For example, the terrorist attacks in Paris of January 2015 triggered a “crucial and urgent need to move toward a European Passenger Name Record (PNR) framework, including intra-EU PNR”.\textsuperscript{582} Threats to security may require restrictions to the exercise of fundamental rights, but one should also consider evaluating the potential harm a limitation of the fundamental right would cause for the values a right aims to protect.

Another illustration of the changing reality of an information society influencing the balancing between rights is the following. Although the ubiquitous availability of information may impact or harm the interest of the data subject protected by the rights to privacy and data protection, its main consequence is that it makes information easier accessible and, hence, does not adversely affect the right to receive information, protected under Article 11 Charter. The ubiquitous availability of information changes the balance between the fundamental rights at stake. The Court of Justice seems to acknowledge this in Google Spain and Google Inc.,\textsuperscript{583} as will be explained in Chapter 5 of this study.

\textit{The EU and the Member States depend on private parties}

Another complicating factor is that governments are increasingly dependent on cooperation with private companies, making it more difficult to hold governments fully accountable for the protection of fundamental rights. Governments engage in partnerships with private companies in order to achieve policy goals they cannot always achieve by themselves.

An example with specific implications is that these companies are regularly required to assist in law enforcement, in particular in criminal law, because in many occasions private

\textsuperscript{580} See Section 6 above.
\textsuperscript{581} Joint statement issued following a meeting of the Ministers of the Interior in Paris, 11 January 2015.
\textsuperscript{583} Case C-131/12, Google Spain and Google Inc., EU:C:2014:317, in particular at 58 and 80. See Hielke Hijmans, “Right to have links removed: Evidence of effective data protection”, Maastricht Journal of European and Comparative Law, 2014(3).
companies rather than the government are in possession of the information that facilitates police work.\textsuperscript{584} This blurs the dividing line between the public and the private sector and is difficult to reconcile with the state monopoly on law enforcement. The result of this practice may be that the constitutional guarantees surrounding law enforcement are insufficiently warranted. Government access to information is usually surrounded by procedural guarantees, laid down in laws on criminal procedure. These constitutional guarantees do not necessarily apply where private companies access information.

Van Dijck mentions the far-reaching risk of joint interests of governments and big companies, which may not necessarily coincide with the interests of individuals to have their rights protected.\textsuperscript{585} She includes the quote: “If Big Brother came back, he’d be a public-private partnership”.\textsuperscript{586}

The dependency of the European Union and its Member States on private parties relates to the shift of power towards companies that is made possible by the asymmetric market structure, with a few dominant players on the internet.\textsuperscript{587} This complicates the effective and legitimate performance of government tasks. We mention two examples where behaviour of big internet companies complicates the full respect of democratic values and fundamental rights.\textsuperscript{588} First, internet users have no or little control over the privacy settings on the internet, notwithstanding the efforts of data protection authorities to influence these.\textsuperscript{589} Second, the market of cloud computing is asymmetric. Most of our personal information is stored in the cloud, posing risks for privacy and data protection, for reasons of security, but mainly because neither internet users, nor professional clients of cloud service providers have control over this information.\textsuperscript{590}

\textit{Conflicts of jurisdiction are an inherent phenomenon on the internet and should be addressed}

The global nature of the internet disregards physical borders and is not bound by national territories. These characteristics are difficult to reconcile with the territoriality principle, which is the most basic principle of international jurisdiction,\textsuperscript{591} and with the jurisdiction of the European Union and its Member States, which is in principle limited to their physical territories. Legitimate interests of EU residents can be directly affected by activities on the

\textsuperscript{584} This is, for instance, the \textit{raison d’être} of the measures on PNR or on data retention.
\textsuperscript{585} José Van Dijck, Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology, Surveillance & Society 12(2), 2014, 197-208, at 203. She mentions alleged connections between Silicon Valley and the NSA.
\textsuperscript{586} Title of a column by Timothy Garton-Ash in The Guardian of 27 July 2014: “If Big Brother came back, he'd be a public-private partnership.”
\textsuperscript{587} See section 5 above.
\textsuperscript{588} This statement reflects potential powers, but is not meant as an accusation of actual bad behaviour of big internet companies.
\textsuperscript{591} Cedric Ryngaert, Jurisdiction in International Law, United States and European Perspectives, KU Leuven, Doctorate Thesis, 2007, at 46.
internet originating from third countries, but the Union and its Member States do not necessarily have jurisdiction to enforce.

Moreover, on the internet positive conflicts of jurisdiction arise in many instances. Reidenberg a.o. even state that questions about jurisdiction arise in almost every internet case. The same activities may trigger jurisdictional claims from up to potentially all states in the world, including states where conflicting legal norms apply. This is problematic: data are ubiquitously available, or in other words, they are everywhere, whereas there is no global convergence on how to deliver protection.

Conflicts of jurisdiction are an inherent phenomenon on the internet and should be addressed, in relation to third countries that do not share the same democratic values, but also with countries that share many of the values that deserve protection. There is no global consensus or even convergence on the arrangements for delivering protection. An illustrative example of differences in approach on how to deliver protection is the diverging way the US and the EU deal with privacy and protection, notwithstanding the fact that they largely share the same values. While in the EU privacy and data protection are fundamental rights under Articles 7 and 8 Charter, in the US data privacy in the private sector is part of consumer law and enforced by the Federal Trade Commission as part of its activities against unfair and deceptive practices. Jurisdictional issues will play an important role in Chapter 9 of this study.

10. Introductory Ideas on How the EU and its Member States could regain Control

Three basic conditions

First, the EU is competent in respect of data protection under Article 16 TFEU and the essential elements of data protection are laid down in primary EU law. Moreover, Chapter 2 concluded that privacy and data protection are constitutional values that matter in an information society. At least in the short term, it is not a viable option to modify the substantive principles of data protection and to look for alternatives, just because some of the principles might appear to be obsolete in the era of big data.

Second, the new circumstances do not alter the fact that individuals remain fully entitled to the protection of their fundamental rights to privacy and data protection under both EU law and national law, in full compliance with the ECHR. The constitutional arrangements of the

---

592 Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law, 30 June 2013, Fordham Center on Law and Information Policy, at 1.
593 Data protection – or data privacy, as it called in the US – is much wider than privacy protected under the US constitution, in particular in the private sector where data protection is part of consumer protection, see Chapter 6, Section 12 of this study.
594 See Chapter 2 of this study.
595 See, on this, Julie Brill, “Bridging the divide”, in: Hijmans and Kranenborg (eds), Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), (Intersentia, 2014), as well as Chapter 7, Section 5 of this study.
European Union and its Member States do not and should not make any distinction between online and offline protection.\textsuperscript{596}

Third, delivering protection is a responsibility of governments, be it national or EU, in a democratic society and under the rule of law. Governments are accountable. This accountability can also be formulated as a positive obligation for governments to ensure that private organisations protect fundamental rights in an effective way, an obligation that has an additional dimension on the internet, if only because of its asymmetric market structure. It must be ensured that fundamental rights are fully effective in horizontal relations.\textsuperscript{597}

\textit{Five directions}

A first direction for ensuring full protection is the interpretation of existing instruments in a way that takes the changed circumstances into consideration. Under current law solutions can be found or, paraphrasing Castells, we can use current law to grasp what is new by referring to the past.\textsuperscript{598} By way of example, in \textit{Google Spain and Google Inc.} the Court of Justice of the European Union showed how to cope with the territorial scope of EU data protection law.\textsuperscript{599} Although in principle the applicability of the law is limited to the territory of the Union and although the law has as its point of departure that data are located in specific jurisdictions, the Court gave a wide interpretation of a notion in Directive 95/46,\textsuperscript{600} based on the objective of effective and complete protection of fundamental rights of persons. The result of the wide interpretation of this notion of “in the context of the activities of an establishment”\textsuperscript{601} was that the Spanish establishment of Google could be held responsible for data processing on the search engine of Google – which is essentially a US company – and EU law could apply.

A second direction is adapting legislative arrangements to the new circumstances and strengthening the protection given in these legislative instruments, which requires innovative thinking on arrangements in view of the extent of the problem. This is a prime objective of the General Data Protection Regulation,\textsuperscript{602} it does not question the substantive principles of data protection, but it envisages the strengthening of enforcement mechanisms. This may include new arrangements for effective governance, where the existing arrangements of

\textsuperscript{596} See also UN Resolution affirming that the same rights that people have offline must also be protected online: UN General Assembly, Human Rights Council, “The promotion, protection, and enjoyment of human rights on the Internet”, Doc. No. A/HRC/20/L.13, 29 June 2012, available through: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx. See also: UN General Assembly plenary on 18 December, 2014, Resolution “Right to Privacy in the Digital Age” (A/RES/69/166), affirming “that the same rights that people have offline must also be protected online, including the right to privacy”.

\textsuperscript{597} This positive obligation to protect was discussed in Chapter 2, Section 7 of this study, in relation to the paradigm of horizontal effect of fundamental rights.

\textsuperscript{598} See Section 2 above.

\textsuperscript{599} Case C-131/12, \textit{Google Spain and Google Inc.}, EU:C:2014:317, in particular at 53.

\textsuperscript{600} Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

\textsuperscript{601} Article 4(1)(a) of Directive 95/46/EC.

legislation, enforcement and judicial control are considered insufficient. It could be argued that the consistency mechanism, as provided for in the proposed General Data Protection Regulation\textsuperscript{603}, is such a new arrangement.

A third direction is addressing the changed relationship between the public and the private sector. The private sector, which includes market players and organisations of civil society, may be involved in the implementation of data protection law and, thus, in the exercise of government tasks. This is usually referred to as multi-level governance.\textsuperscript{604} Cooperation with the private sector is needed, but this has – constitutional – limits, in particular where companies are required to assist in law enforcement. Since governments are increasingly dependent on private parties there is a need to examine this trend from the perspective of democratic legitimacy and accountability.

A fourth direction for the European Union and its Member States is focusing their interventions on essential components of privacy and data protection, for pragmatic and for jurisdictional reasons. When addressing the challenges to privacy and data protection on the internet, it may prove necessary to focus and to distinguish between legal provisions and underlying values, allowing a differentiation in the level of protection guaranteed under EU law. Such a differentiation is worth considering for pragmatic reasons – one cannot deal with all challenges at the same time – but also for jurisdictional reasons – one should not claim jurisdiction with external effect for too wide a range of protection, which may not always represent essential values in a democratic society. In the relationship between the Union and its Member States a similar reasoning may apply: where values are of a more essential nature a widely shared protection can be given at the EU level, without leaving too much room for exceptions and limitations based on national particularities.

A fifth direction would be addressing the values themselves. As explained, the main features of the internet and the development of communications on the internet challenge some principles in the legal system of privacy and data protection. The core principles of data protection are laid down in Article 8 Charter and represent the core of EU fundamental rights protection. Also, where principles are not laid down at the level of the Treaties – and where the EU legislator has flexibility – there are no intentions to adapt the substantive principles of data protection by the EU legislator. The General Data Protection Regulation does not intend to touch key principles, for good reasons as explained in various parts of this study. However, this does not mean that all principles are set in stone, even in the long term perspective.

11. Conclusions

Privacy and data protection are fundamental rights that must be respected in a democratic society that is subject to the rule of law. These fundamental rights are challenged in our

\textsuperscript{603} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. See mainly Chapter VII of the proposal.

\textsuperscript{604} Further read: Special issue on the Constitutional Adulthood of Multi-Level Governance, Maastricht Journal of European and Comparative Law 2014, Vol. 21, No. 2.
information society. These challenges justify that governments in general and the European Union under Article 16 TFEU in particular give priority to addressing the main issues raised in the information society in a legitimate and effective way.

The internet causes the perception of a loss of control over personal data and of a lack of certainty. Castells observes: “We live in confusing times, as is often the case in periods of historical transition between different forms of society.” For the European Commission, the rapid pace of technological change and globalisation provide incentives to reform the data protection framework. Prins argues that governments lack overview in our complex and rapidly evolving societies – with an ever greater role for technology. (Section 2)

The internet is a single unfragmented space with a loose governance structure. This structure is not uncontroversial, for instance in relation to the responsibilities for the integrity of the system, the continuity of the services and security threats. The internet has a societal function, which is difficult to reconcile with its qualification as “the largest experiment involving anarchy in history, the world’s largest ungoverned space”.605 However, too much government involvement in the public infrastructure of the internet increases the risk of barriers to the free flow of information across the globe being imposed. (Section 3)

As a networked society the internet is a highly dynamic and open structure. This structure is a trigger for innovation and growth, but networked societies are vulnerable, also for security reasons. Fragmentation of the internet has connotations such as an EU cloud, a BRICS Internet or a halal internet and is seen as a threat for the internet. Considerations of privacy and data protection could justify measures that result in fragmentation, but do not justify measures adversely affecting democracy on the internet. (Section 4)

A free internet is a common good, yet it is under threat. Where big companies and governments exercise power on the internet, a counterpower must protect the rights of individuals, ensuring that individuals can effectively exercise their rights. Six phenomena challenge the mandate of the European Union under Article 16 TFEU: uncertainty, lack of transparency within governments and internet players, security threats, increased visibility of individuals, automated decision-making and an asymmetric market structure. (Section 5)

Big data justifies a qualitative shift in thinking. It can enhance the quality of decision-making in an unprecedented way, to the benefit of society, but it is also pervasive in the daily life of individuals. Big data has a societal impact, because of two main reasons: it enables unprecedented predictions on private lives and it shifts power to those who hold information and those who supply it. As Kohnstamm says, personal freedom should not be defined by what businesses and governments know about individuals. (Section 6)

People can no longer evade surveillance through electronic means. This is the genuinely new dimension of this type of surveillance, related to the role now played by the internet in our daily lives. The study distinguishes between surveillance by states and surveillance by private

companies, between mass surveillance and targeted surveillance and, more relevant for surveillance by states, between internal and foreign surveillance. It is the massive scale of surveillance that leads to the most serious breaches of fundamental rights. (Section 7)

Targeted surveillance is not necessarily less intrusive than mass surveillance, because it may be based on discriminatory criteria and the result may be stigmatisation. The democratic legitimacy and accountability of surveillance is at stake, due to secrecy and the cooperation of the private sector in government surveillance. This blurring dividing line between the public and private sectors is difficult to reconcile with the state monopoly on law enforcement. Cooperation by companies in this area also carries risks for the constitutional guarantees surrounding law enforcement (Section 8).

More generally, the internet changes the perspective of the European Union and its Member States. The governance structure of the internet is an example of the declining role of the state. The reality of the internet is difficult to reconcile with core data protection principles such as ‘consent’ and ‘purpose limitation’, and also influences the balancing with other interests since fundamental rights and public interests increasingly coincide. The Union and its Member States are becoming more dependent on private parties resulting in a shift of power towards big companies on the internet. Conflicts of jurisdiction are an inherent phenomenon on the internet and should be addressed (Section 9).

The study mentions five directions for the European Union and its Member States to regain control. First, the existing legal instruments for privacy and data protection should be interpreted in a way taking the changed circumstances into consideration. Second, the legislative arrangements should be adapted to the new circumstances. Third, the changed relation between the public and private sectors should be addressed by recognising a closer involvement of the private sector in the implementation of the law, but without questioning the final responsibility of government. Fourth, the Union and its Member States should focus their interventions on essential components of privacy and data protection, for pragmatic and for jurisdictional reasons. Fifth, the Union and its Member States could reconsider the main principles of data protection, in order to adapt these principles to the changed circumstances, however without giving up on the need for protection of individuals. This last direction can only become relevant in the long term perspective, if only because the main principles of data protection are laid down in primary EU law, i.e. at the constitutional level. These directions are useful to keep in mind in exercising the roles under Article 16 TFEU. Obviously, they are guiding for the EU legislator. (Section 10)
Chapter 4. The Mandate of the EU under Article 16 TFEU and the Perspectives of Legitimacy and Effectiveness

1. Introduction

The Treaties of the European Union recognise privacy and data protection as fundamental rights of a constitutional nature, reflecting essential values in a democratic society under the rule of law. The Union has a specific and broadly formulated mandate to ensure the protection of all individuals, laid down in Article 16 TFEU, that enables the Union to address the perceived loss of control over personal data on the internet and to regain control. Since we are dealing with global and technologically difficult challenges and effective protection of individuals in the Union cannot be achieved by the Member States acting alone, more Europe makes sense.606

This chapter analyses the research question’s general elements on the role of the European Union under Article 16 TFEU, linking the object of protection and the challenges posed by the internet,607 on the one hand, to the contributions of the various actors, on the other hand.608 This analysis includes the following subjects:

a. The general design of the EU mandate, with the Member States as important actors;
   b. A shared competence and the subsidiarity and proportionality principles;
   c. Limitations to EU competence and decentralised implementation of EU law;
   d. The legitimacy of EU action, the EU citizens and the crisis of social legitimacy;
   e. The legitimacy of EU action, the Member States and the pluralist legal context;
   f. Legitimacy based on output;
   g. Effectiveness and delivering privacy and data protection on the ground.

The first objective of the chapter is to define the mandate’s scope and limitations, as well as the roles of the Member States. The second objective is to analyse how the European Union can exercise its mandate in a legitimate and effective manner, providing a general framework for the analysis of the instruments that enable the various actors to contribute to the protection, and formulating some basic requirements for these contributions.609

Section 2 introduces the general design of the mandate, which recognises that the Member States remain important actors, although with limited discretionary powers. Section 3 gives a first specification of the mandate under Article 16 TFEU, by analysing the conferral of a broad competence, which is a competence shared with the Member States, and by giving an outline of the three tasks of actors under Article 16 TFEU. This is followed in Section 4 by an explanation of the role of the principles of subsidiarity and proportionality. There are further limitations to the exercise of the EU mandate. The European Union should respect national

---

606 Wording taken from Article 5(3) TEU (the principle of subsidiarity).
607 Chapters 2 and 3.
608 Chapters 5-8.
609 Chapter 9 deals with the external aspects of Article 16 TFEU, in the international context.
identities whilst safeguarding national security, and cultural differences. This study argues that the exception for national security is more limited than appears to be the case at first sight (Section 5). Further limitations result from the organisational structure of the Union: the rule is decentralised implementation, enforcement and organisation of the judicial protection (Sections 6 and 7).

Citizens may expect to be protected effectively by the European Union, but at the same time they want the often quoted democratic deficit of the Union to be addressed. Democratic shortcomings of and lack of support for the Union are matters of concern, in particular because the wide powers afforded to the Union on data protection under Article 16 TFEU delimit the discretion of democratically legitimised national governments, in connection to fundamental rights protection. The various aspects of legitimacy of EU action are the subject of Sections 8-13.

Legitimacy and effectiveness are addressed in Sections 14 and 15. Effectiveness and legitimacy are closely linked for two reasons: first, effectiveness is a constitutive element of legitimacy (‘output legitimacy’) and second, considerations of democratic and judicial legitimacy (‘input legitimacy’) may limit what would in theory be the most effective outcome. Effectiveness as a separate requirement is explained as delivering privacy on the ground. Section 16 contains the conclusions.

Taking its inspiration from a quote of Weiler stating that the Union “is neither a nation nor a state, yet it is certainly governed in accordance with a system of fundamental principles”, this chapter shifts the focus to the governance aspects of privacy and data protection. It formulates the points of departure for the next chapters of this study which will discuss the respective contributions of the Court of Justice of the European Union, the EU legislator and the supervisory authorities to the respect of privacy and data protection under EU law. The findings in this chapter are meant to outline preconditions for these specific contributions.

2. A General Design of the Mandate under Article 16 TFEU: The Member States are Important Actors

Article 16 TFEU reads as follows:

“1. Everyone has the right to the protection of personal data concerning them.  
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.  
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.”

610 Joseph Weiler, Do the new clothes have an emperor? and other essays on European integration, Cambridge University Press 1999, at viii.
Privacy and data protection constitute a domain where the competence of the European Union to protect individuals is laid down in Article 16 TFEU as a positive obligation for the Union to ensure protection. Article 16 TFEU is closely related to Articles 7 and 8 Charter, which specify that privacy and data protection are fundamental rights that must be respected where EU law applies.\(^{611}\)

The mandate of the Union has a general dimension, since the Union is based on values and the Treaties are ambitious in promoting these values, also in the wider world as illustrated by the Treaty on the European Union, on which the Union is based.\(^{612}\) The EU mandate has particular relevance on the internet, since privacy and data protection prove to be constitutional values that matter in an information society. However, the protection of these values is at risk in view of the features of the internet and the development of communications on the internet, leading to a loss of control illustrated by phenomena such as big data and mass surveillance. Effective protection is needed because individuals are entitled to it, yet the protection also enhances the trust in the Union and more in general in governments.\(^{613}\)

Article 16 TFEU delineates three specific tasks that must enable the European Union and the various actors within the Union to deliver protection. Article 16(1) TFEU, read in combination with Articles 7 and 8 Charter, implies that the European Court of Justice has the task to ensure that these rights are respected, under the rule of law. Article 16(2) TFEU specifies the task of the Council and the European Parliament to adopt data protection legislation. Additionally, Article 16(2) TFEU obliges the Union to give the independent data protection authorities the task of ensuring control of the rules on data protection. The task of these authorities is also mentioned in Article 8(3) Charter.

The last sentence of Article 16 TFEU is not addressed. It contains a reference to rules on data protection in Article 39 TEU in relation to the common foreign and security policy. Article 39 does not play a significant role in practice, in the absence of EU legislation in this policy area relating to the processing of personal data and in the absence of legislation or proposed legislation based on Article 39 TEU. However, the findings of this study apply mutatis mutandis also to Article 39 TEU.

The context: Article 16 TFEU gives a mandate to the EU, but the Member States remain important actors

Article 16 TFEU confers wide powers on the European Union to act in the domain of privacy and data protection. However, it is a competence which the Union shares with the Member States and which it exercises with due regard for the principles of subsidiarity and proportionality.

\(^{611}\) Because of the limited scope of the Charter, as will be further explained in Chapter 5.\(^{612}\) E.g., in Articles 2, 3 and 21 TEU.\(^{613}\) See Chapter 2.
In all three tasks under Article 16 TFEU the Member States have a role. The first task results from Article 16(1) TFEU which specifies that everyone has the right to the protection of his or her personal data. Ensuring respect for this right to data protection is primarily undertaken within the legal systems of the Member States, ultimately subject to review by the Court of Justice of the European Union. The second task is laid down in Article 16(2) TFEU, first sentence, and requires the adoption of rules under the ordinary legislative procedure, by the EU legislator, the Council and the European Parliament; yet, there is room for national legislation. The third task is laid down in the second sentence of Article 16(2) TFEU and comprises control of the rules, by independent supervisory authorities which are foremost national authorities.

The power of the European Union under Article 16 TFEU coincides with competing competences of Member States. An example is the freedom of expression where the Union does not have competences comparable to those laid down in Article 16 TFEU. Furthermore, the Union lacks certain powers in relation to national security, whilst the enforcement of EU law is mainly decentralised and must be ensured by the Member States.

Article 16 TFEU and the proposals based on this article – particularly the proposed General Data Protection Regulation – are not evident choices in the current state of EU law. Several arguments plead against using Article 16 TFEU as a basis for an overarching regulation on data protection in the European Union. This study refutes or, where relevant, nuances those arguments.

**Legitimacy and effectiveness: perspectives for understanding the mandate of the EU**

Legitimacy and effectiveness add new perspectives to the complicated reality of privacy and data protection on the internet. Legitimacy and effectiveness are different issues, but – as explained in this chapter – they are to a certain extent interlinked, if only because legitimacy can be measured in terms of effectiveness. The objective of effective protection in itself creates legitimacy. This is what is usually called ‘output legitimacy’. Output legitimacy is opposed to ‘input legitimacy’, the democratic legitimacy of government action. Input legitimacy is particularly important in view of the democratic shortcomings of the European Union itself and because of the involvement of actors, notably the independent data protection authorities, who are not accountable for their performance to elected bodies. As will be explained, effectiveness of protection (output legitimacy) is not sufficient for trust; democratic legitimacy (or input legitimacy) is also required.

---

614 As specified in Chapter 6, Section 6.
615 Under Article 28 of Directive 95/46.
616 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.
The legitimacy of the European Union in the governance of privacy and data protection is understood as: ensuring that there is some degree of accountability towards political institutions. The Union’s democratic shortcomings affect the legitimacy of and support for the Union, also because the exercise of powers by the Union in the domain of fundamental rights has a direct impact on individuals and limits the scope for decision-making by national governments which are no longer capable to protect their citizens according to national preferences, subject to democratic and judicial accountability in the national legal order. As will be explained below, the Union operates in a pluralist legal context and needs to take account of the legitimate interests of its main interlocutors: individuals and Member States.

Since this is a legal study it focuses mostly, but not fully, on legitimacy in a formal sense and not on more social aspects of legitimacy of the Union. A social aspect of legitimacy is for instance the question whether the absence of a European demos or – possibly connected to this – the low turn-out in elections for the European Parliament diminishes the legitimacy of EU action.

Another perspective is effectiveness, a requirement for all action within the scope of EU law. EU action in the domain of privacy and data protection on the internet must be effective, which this study specifies as: ensuring protection by bridging the gap between principles and practice. Effectiveness requires the use of the most suitable instruments, if only not to lose the trust of citizens. Here we note the declining effectiveness of traditional government intervention, as such, and the fact that other forms of governance are emerging, for instance cooperation with non-governmental institutional stakeholders, in particular the private sector and civil society.

3. A First Specification of the Mandate under Article 16 TFEU: Broad Powers of the EU, but a Shared Competence, and an Outline of the Three Tasks

The division of competences between the European Union and the Member States is one of the essential and difficult issues of EU integration and plays an important role in this study. This division is determined by the principle of conferral laid down in Article 5(2) TEU.

---

619 See Chapter 1, Section 2.
621 The relation with a third category of main interlocutors – third countries and international organisations – will be discussed in Chapter 9 on the external relations of the Union.
622 The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press, 1999, e.g at 80.
625 See, e.g., Chapter 6, Sections 12-14.
subject to the provisions of the Treaties, and, where the Union is competent to act and has acted, by the primacy or supremacy of EU law. Article 5(2) TEU also affirms that competences not conferred upon the Union in the Treaties remain with the Member States.

**Wide powers of the EU in privacy and data protection**

Article 16 TFEU confers wide powers on the European Union to act in the domain of privacy and data protection. In doing so, Article 16 TFEU goes beyond the role of the Union in respect of most other fundamental rights under the Charter as delimited in Article 51(2) thereof. Where the Charter does not establish “any new power or task for the Union, or modify powers and tasks as defined in the Treaties”, Article 16 TFEU precisely establishes a power of the Union in relation to privacy and data protection. Article 16 TFEU also means that privacy and data protection fall, by definition, within the scope of EU law. This is the necessary corollary of the Union’s mandate to ensure the protection of everyone’s rights.626

Article 16 TFEU has a further consequence. The Charter – including Articles 7 and 8 thereof – only applies to the Member States where they act within the scope of EU law. This limitation of scope of the Charter is laid down in Article 51(1) Charter. The consequence of Article 16 TFEU is that this limitation of the applicability of the Charter is no longer relevant in the domain of privacy and data protection. Where the Member States act in this domain, they act by definition within the scope of EU law and the Charter is applicable.

**Article 16 TFEU is a shared competence, but in practice complete**

The Treaty of the Functioning of the European Union contains catalogues of areas where the Union has exclusive competence, where it shares competence with the Member States and where it may act to support, coordinate or supplement Member State action.627 Shared competence is the main rule:628 exclusive competences as well as supporting, coordinating and supplementing competences are listed in an exhaustive way, whereas in all other areas the competences are shared. These catalogues are not only intended to clarify the EU competence, but also to contain this competence, to avoid a creeping expansion of EU competence or an encroachment on the exclusive areas of competence of the Member States.629

This study assumes that Article 16 TFEU can be considered a shared competence, although this is not explicitly mentioned in the Treaty. The assumption is based on a logical reading of

---

626 This understanding has as a further consequence that the addition “within the scope of EU law” in Article 16(2) TFEU, in relation to processing by the Member States, would be without meaning. On the text of Article 16(2) TFEU, see Chapter 6, Section 2 of this study.
627 Articles 3, 4 and 6 TFEU.
the TFEU. Out of three catalogues of competences, two are exhaustive, whereas the catalogue of shared competences in Article 4 TFEU contains an enumerative list. Data protection is not mentioned in any catalogue of competences, hence it belongs to the only ‘open’ catalogue.

Article 2(2) TFEU specifies what shared competence means: both the European Union and the Member States may legislate and adopt legally binding acts in that area. However, the Member States shall exercise their competence only to the extent that the Union has not exercised its competence. Timmermans calls this ‘diplomatic drafting’. The Treaty aims to state that Member States shall not exercise their power to the extent the Union has exercised its competence.630 Legislative instruments of the Union, once adopted and entered into force, have a blocking effect on the competences of the Member States. This goes quite far. Member States no longer have competence to legislate, even if they do it in a way that is not in conflict with the instrument of EU law, but only complements this instrument.631 Article 2(2) TFEU is a rule of competence, not of conflict. The Member States’ competences revive where EU instruments no longer exist.632

Protocol (No 25) on the exercise of shared competence further specifies that “when the Union has taken action in a certain area, the scope of this exercise of competence only covers those elements governed by the Union act in question and therefore does not cover the whole area”. In short, under Article 16 TFEU Member States remain competent on elements where the Union has not exercised its competence.633 The difficulty of Article 2(2) TFEU and Protocol (No 25) is the interpretation of the remaining autonomy of the Member States, in areas where the European Union has exercised its competence. It is not always clear which elements are covered by an EU instrument and consequently where there is no more room for Member States’ action. This is a relevant issue in relation to Article 16 TFEU and the exercise of powers on the basis of this article. The competence of the Member States on data protection is limited to elements not covered by the Union acts, currently Directive 95/46 on data protection and other EU instruments on data protection.634 The Member States’ room for manoeuvre is reduced, as the ruling of the European Court of Justice in ASNEF and FECEMD635 illustrates. The Court denied that the Member States retained competence to specify a provision of Directive 95/46. This room for manoeuvre will be further reduced after the entry into force of the General Data Protection Regulation.636

---

632 These instruments can be limited in time or repealed by the legislator. Member States competence also revives where an EU instrument is annulled by the CJEU, as was the case with Directive 2006/24 (data retention) in Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitinger (C-594/12), EU:C:2014:238.
634 This issue must not be confused with powers given to Member States in an EU act to adopt additional rules. See on this: European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at II.2.a, on the relation between powers given to Member States in an EU act to adopt additional rules.
635 Joined cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777, relating to Article 7(f) of Directive 95/46.
To be complete, the European Union possibly has an exclusive competence to conclude international agreements on data protection, under Article 3(2) TFEU. The Union has exclusive competence in a number of situations, for instance where this “is necessary to enable the Union to exercise its internal competence, or insofar as its conclusion may affect common rules or alter their scope.”

An outline of the three tasks of the EU under Article 16 TFEU

The task of ensuring – under Article 16(1) TFEU – that everyone’s right to data protection is respected is not necessarily a competence of the Union. The Member States are important actors, if only because most data processing takes place within the national jurisdiction, either by authorities of the Member States or by the private sector. However, EU law determines the result – the guarantee that everyone’s right is effectively protected – and the Court of Justice of the European Union is the institution ultimately supervising the acts of the Member States. To be complete, where the processing of personal data takes place within the remit of the EU institutions and bodies, they must guarantee effective protection, without involvement of the Member States.

The task of the EU legislator – under Article 16(2) TFEU, first sentence – is necessarily a competence of the Union. The EU legislator must lay down the rules relating to the protection of individuals with regard to the processing of personal data, in full compliance with the Charter. This formula is unconditional: the European Parliament and the Council shall lay down the rules. This, in principle, does not leave room for national law in this area.

The present rules – predating the Lisbon Treaty – do not cover the whole area of EU competence and do not fully comply with Article 16 TFEU. One shortcoming is the limited scope of application of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which leaves data protection in the police and judicial sector in domestic situations to national law. Article 1(2) of this framework decision excludes personal data that have not been transmitted or made available between Member States. In short, in cases where only

---

637 Article 3(2) TFEU reads as follows: “The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.” See further Chapter 9.

638 Mainly subject to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.

639 Italics added by author.

640 In principle. As explained in Chapter 6 certain elements of data protection should be left to the Member States.


police or judicial authorities of one Member State are involved the Framework Decision does not apply.

The reform of the data protection framework, which will replace the present EU rules on data protection such as Directive 95/46, must ensure that the EU legislator fulfils its obligation under Article 16(2) TFEU. As a consequence of the fulfilment of this obligation of the Union, the Member States are no longer competent to lay down rules on data protection, notwithstanding the fact that the EU legislator may – explicitly or implicitly – delegate tasks to the Member States.

The task of ensuring – under Article 16(2) TFEU, second sentence – that compliance with these rules shall be subject to control by independent authorities is primarily a task of the EU legislator. As part of the rules on data protection, the EU legislator must lay down the conditions for control by these authorities. Article 28 of Directive 95/46 on data protection contains such conditions. This is the consequence of qualifying control by the authorities as “an essential component of the protection”, as confirmed in the case law of the European Court of Justice. Presently, these authorities are mostly public authorities of the Member States. Article 16 TFEU seems to recognise this reality, since it mentions the authorities in plural, in contrast to Article 8 Charter.

In short, Article 16(2) TFEU, second sentence, provides for a system of effectively shared competence, where the main tasks of the authorities are defined by the EU legislator, but their organisation remains a national competence, at least to the extent that this competence is not limited by a provision of EU law. EU law determines the result. The case law of the Court in three infringement cases on the independence of data protection authorities in Germany, Austria and Hungary confirms this role of EU law.

Summing up, data protection has become a concern of the European Union, although the implementation is shared with the Member States. The Member States have competence to ensure that the right to data protection – a right under EU law – is respected, but it is the EU

---

643 With a prominent position for the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. In this context we also mention the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.

644 The present rules predate the Lisbon Treaty and have different legal bases. Since they do not cover the whole area of EU competence, it is argued that present law does not fully comply with Article 16 TFEU (see also Chapter 6, Section 2 of this study).

645 Chapter 6 of this study will explain this further.

646 Chapter VI of the Commission Proposal for a General Data Protection Regulation (COM (2012), 11 final) contains more precise conditions.

647 Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, as most recently confirmed in Case C-362/14, Schrems, EU:C:2015:650, at 42. See Chapter 7, Sections 1 and 2.

648 See, mainly Chapters 7 and 8 of this study.

649 Cases C-518/07, Commission v Germany, EU:C:2010:125, C-614/10, Commission v Austria, EU:C:2012:631 and C-288/12, Commission v Hungary, EU:C:2014:237. See Chapter 7, Section 9 of this study.
legislator that adopts the legislation in this area. The control by independent authorities is effectively a shared competence, with the understanding that EU law determines that there shall be control.

4. The Exercise of the Mandate under Article 16 TFEU should comply with the Principles of Subsidiarity and Proportionality

Where powers are conferred on the European Union, as is the case in Article 16 TFEU for data protection, EU action must respect the principles of subsidiarity and proportionality. These principles are used as instruments for demarcating the competences of the Union and the Member States and also as instruments to impose restraints on the legislative activity of the Union. In practice, these principles mainly serve to restrain the Union. As Craig & de Búrca state, they reflect the “shift away from hierarchical governance, and away from the dominance of top-down EU action”.

Testing EU data protection action on subsidiarity and proportionality

The test of subsidiarity under Article 5(3) TEU entails two main elements. The first element is that the European Union can only act if the objectives of an action cannot be sufficiently achieved by the Member States. Subsidiarity expresses a preference for a national or decentralised approach. To ensure that this preference is taken seriously, EU law foresees a close involvement of national parliaments in the legislative procedure of the Union. The second element expresses the need for efficiency and effectiveness. Implementation of this second element takes place through obligations for the European Commission to consult widely before an act is proposed and by specific requirements as to the justification of proposals.

The Commission justifies the proposed General Data Protection Regulation in light of subsidiarity by emphasising that “personal data are transferred across national boundaries, both internal and external borders, at rapidly increasing rates”. In relation to the mandate of

652 This reads: “Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level”.
653 “It must be considered whether the objective of the proposed action could be better achieved at EU level”, Case C-508/13, Estonia v European Parliament and Council, EU:C:2015:403, at 45.
654 Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality, annexed to the Lisbon Treaty, in particular Articles 6 and 7, which include the ‘yellow card’ procedure.
the EU legislator under Article 16(2) TFEU, this study argues that efficient and effective privacy and data protection on the internet cannot be sufficiently achieved by the Member States. This is a subject matter that, in general, can be better regulated at Union level, if only because of the inherent cross-border effects of the action, both within and outside the EU territory, in compliance with the second element of the principle of subsidiarity.

This argument does not necessarily mean that all legislation on data protection should be adopted at EU level, also considering the preference for constraint of EU action as mentioned above. In the legislative procedure on the proposed General Data Protection Regulation the Council discussed whether processing activities by the public sector should not better be regulated on the national level and, therefore, better not be incorporated in an EU Regulation.657 This is a valid discussion, in particular because the objective of creating a level playing field on the internet in the context of the digital single market does not directly apply to the public sector.

This study takes the view that there are convincing arguments not to exclude the public sector from the General Data Protection Regulation. For the individual who is entitled to protection it should not make a difference whether his or her data are processed by the private sector or by the public sector. Moreover, the boundary between the public and the private sectors is not always clear and different in each Member State.

The outcome of the discussion in the Council was a proposal to include a provision in the General Data Protection Regulation allowing Member States to maintain or introduce more specific provisions, for instance “with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.658

Subsidiarity is closely linked to the principle of proportionality,659 laid down in Article 5(4) TFEU and providing that “content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties”.660 The principle of proportionality entails that the action should be necessary to achieve the objectives of the Treaties. As a consequence, the discussion focused on the choice of instruments, assessing the perceived prescriptive nature of the proposed General Data Protection Regulation under the principle of proportionality.661 In light of the phenomena mentioned above, EU action aiming at the

659 According to Craig & de Búrca this distinction is blurred and both principles are used together, EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, at 168-169.
660 This is proportionality as it is meant in this section. The principle is also used in other contexts, e.g., in the context of the limitation of fundamental rights.
661 Particularly the discussions relating to the risk-based approach that should replace prescriptive provisions. See, e.g.: Statement of the Article 29 Working Party on the role of a risk-based approach in data protection legal
protection of fundamental rights on the internet could *a priori* be considered a proportionate means to regain control over activities affecting those rights. Of course, this is only the starting point. Each specific EU action in this area will be subject to a proportionality test.\textsuperscript{662}

For the purpose of this study, the importance of subsidiarity and proportionality is that these principles shape the exercise of the competence of the European Union under Article 16 TFEU. In short, Article 16 TFEU has conferred powers to the Union to ensure data protection and the use of these powers complies – as said *a priori* – with the principles of subsidiarity and proportionality. EU action should, in principle, give an appropriate answer to the phenomena on the internet that challenge privacy and data protection.

*Member State competences in competing areas*

As will be explained below, the mandate of the European Union on privacy and data protection concerns a sensitive subject area close to the citizen. However, data protection guaranteed by EU law is not an isolated area and the exercise of the EU mandate has an impact on core competences of Member States. The competence of the Union under Article 16 TFEU coincides with the exercise of other, sometimes competing competences of Member States’ governments. Member States may expect that the Union’s exercise of its competences under Article 16 TFEU does not unduly interfere with their autonomous powers, be it in the area of fundamental rights or in other affected areas of state intervention.

The area of data protection interferes with other fundamental rights as well as with the task of governments to ensure the physical security of individuals. These are areas where the Member States play a key role in the absence of a legal basis for the European Union to act, comparable to Article 16 TFEU. Moreover, privacy and data protection are cross-cutting issues which are relevant in all areas of government intervention where the processing of personal data plays a role.

**5. Security Agencies could be covered by EU Data Protection despite the Limitations to EU Competence in respect of National Identities, National Security and Cultural Differences**

In certain essential domains of government intervention the European Union lacks power. An important limitation to the Unions’power is laid down in Article 4(2) TEU, which not only declares that the Union shall respect essential state functions, but also lays down that national security remains the sole responsibility of each Member State.

*The national identities of the EU Member States*
Article 4(2) TEU requires the European Union to respect the national identities of the Member States. The national identities of the Member States are connected to their fundamental political and constitutional structures and to their essential state functions, which includes ensuring territorial integrity, maintaining law and order and – as will be elaborated below – national security.

The concept of national identity of the Member States played a role in Sayn-Wittgenstein, a case concerning the entry in the civil register of the family name of a person of nobility. The Court of Justice of the European Union stated that “it must be accepted that, in the context of Austrian constitutional history, the Law on the abolition of the nobility, as an element of national identity, may be taken into consideration when a balance is struck between legitimate interests and the right of free movement of persons recognised under European Union law”. The Court referred explicitly to Article 4(2) TEU.

The Sayn-Wittgenstein case may be seen in its specific context, but more in general the respect of national identity is reflected in basic organisational principles such as the decentralised enforcement of EU law and the national procedural autonomy, discussed below. In the context of Article 16 TFEU these elements play a role, for instance where the proposed General Data Protection Regulation describes the tasks of the national data protection authorities in precise terms.

Also the case law of national constitutional courts gives an indication of what national identity encompasses as a legal notion. Von Bogdandy & Schill summarise this case law as follows. The European Union should exercise its powers without infringing certain fundamental constitutional principles, in particular the statehood of Member States, as well as key elements of democracy, the rule of law and fundamental rights.

The ruling in Sayn-Wittgenstein and the paper of von Bogdandy & Schill show that there is a domain where the European Union should take choices of Member States into consideration where they relate to issues which are regarded as being fundamental to national identity. This does not mean that the key elements of the right to data protection should be left to the Member States, if only because these elements are laid down in the Charter, which is an instrument of primary EU law. It does mean however that, on the basis of Article 16 TFEU, EU law should take certain justified interests of Member States into consideration.

663 And, irrelevant in the context of this study, the equality of Member States.
665 Case C-208/09, Sayn-Wittgenstein, EU:C:2010:806, at 83.
666 The person concerned was a Fürstin, princess in English. The registry did not enter her as princess, but just with her normal name.
667 Albeit only in a subsidiary way (ruling, at 92).
669 This will be elaborated in Chapters 7 and 8.
671 Case C-208/09, Sayn-Wittgenstein, EU:C:2010:806.
The notion of national security, in relation to public security and state security

Article 4(2) TEU does not only declare that the role of the Member States in safeguarding national security shall be respected, but takes it a step further: national security remains the sole responsibility of Member States. This limitation of EU competence is of particular relevance to the subject of this study, not in the least because of the relation to the Snowden revelations on the activities of security services.

In order to understand Article 4(2) TEU, this study shall attempt to specify the scope of the exception of national security, in the absence of case law of the European Court of Justice providing a definition of this notion. This is a complicated area since the Treaties empower the European Union in areas which have a direct impact on national security, despite Article 4(2) TEU. Examples in the Treaties are Article 75 TFEU, which provides a legal basis for EU legislation on certain aspects of the prevention and combat of terrorism and related activities, and Article 24(1) TEU, specifying that the Union’s competence in matters of common foreign and security policy shall cover all areas of foreign policy and all questions relating to the Union’s security.

Also, secondary EU law does not give a clear answer. In secondary law, the notions most closely related to national security seem to be public security and state security. Both notions are included in Directive 2004/38 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, and have led to recent rulings of the Court of Justice of the European Union. Article 27 of this directive recognises public security as a ground for the restriction of free movement, in case of a qualified threat to society, whereas state security is recognised as a ground for not informing persons of the grounds of decisions taken against them, in Article 30 of this directive.

In Tsakouridis, the European Court of Justice ruled that public security “covers both a Member State’s internal and its external security”. In the same case, it was “held that a threat to the functioning of the institutions and essential public services and the survival of

---

672 See on this subject also: Article 29 Data Protection Working Party, Document on surveillance of electronic communications for intelligence and national security purposes, Adopted on 5 December 2014, WP 228.
673 Under Article 75 TFEU the European Parliament and the Council “shall define a framework for administrative measures with regard to capital movements and payments, such as the freezing of funds, financial assets or economic gains belonging to, or owned or held by, natural or legal persons, groups or non-State entities”.
674 Also because texts are not always clear. E.g., Article 3(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1, stating: “public security, including the safeguarding of national security and defence”.
676 Case C-145/09, Tsakouridis, EU:C:2010:708, at 43.
the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security.”

This formula resembles to a certain extent the essential state functions mentioned in Article 4(2) TEU.

In P.I. the Court of Justice of the European Union extended this notion to “fundamental interests of society”, which could also include a threat that was not addressed to the calm and physical security of the population as a whole or a large part of it, since in the P.I. case the concrete threat (of child abuse) had only materialised in the family sphere.

The issue of who determines the meaning of public security is relevant as well. The European Court of Justice noted in P.I. that “European Union law does not impose on Member States a uniform scale of values as regards the assessment of conduct which may be considered to be contrary to public security.” However, in the same case the Court adds that the scope of the notion of public security should be controlled by the EU institutions. The Court makes a link to Article 83(1) TFEU that lists a number of particularly serious crimes in respect of which the EU legislature may intervene in the context of the judicial cooperation in criminal matters. In short, the Member States have some discretion, but their discretion is limited.

State security is a notion that is equally included in Directive 2004/38 and its use was scrutinised in ZZ, a case essentially dealing with the use of secret evidence and the dissimulation of the grounds which constitute the basis of a decision taken against the person concerned. State security is a stricter notion than public security and it is even closer linked to national security. The European Court of Justice maintains a high standard for allowing the use of secret evidence. The Court accepts two grounds for non-disclosure of evidence: disclosure must endanger the life, health or freedom of persons or “reveal the

---

678 Case C-145/09, Tsakouridis, EU:C:2010:708, at 44. The CJEU also noted that “objectives such as the fight against crime in connection with dealing in narcotics as part of an organised group are necessarily excluded from that concept”, at 45.


681 This requirement was mentioned in Case C-145/09, Tsakouridis, EU:C:2010:708, at 47. However, in P.I. the CJEU seems to drop this.


683 Case C-348/09, P.I., EU:C:2012:300, at 23.


687 This use of evidence limits the rights of individuals under Article 47 Charter (effective remedy and fair trial). The case relates to the jurisprudence in Kadi and Al Barakaat (see, e.g., Chapter 2, Section 5 of this study).

688 If only because of the wording of Article 30(2) of Directive 2004/38: “The persons concerned shall be informed […] of the […] public security […] grounds on which the decision taken in their case is based, unless this is contrary to the interests of State security.”
methods of investigation specifically used by the national security authorities and thus seriously impede, or even prevent, future performance of the tasks of those authorities.”

Arguably, ZZ demonstrates that state security, as just described, cannot be meaningfully distinguished from the notion of national security under Article 4(2) TEU, in view of the fact that both notions are inextricably related to the activities of intelligence agencies. This would mean that there is EU competence in this domain, at least to determine the scope *ratione materiae* of national security (or state security).

The Court of Justice of the European Union gives further guidance in ZZ on the extent of EU competence in relation to state security,690 where it rules: “Although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns state security cannot result in European Union law being inapplicable.” In itself, the ZZ case demonstrates that justifying a national procedure on the grounds of state security (or national security) does not bring this procedure outside of the scope of EU law. This reasoning is in line with earlier case law where the Court ruled that there is no general exception excluding measures taken for reasons of – public – security from the scope of EU law. Such an exception would render EU law ineffective.692

In the case of ZZ a national security exception was invoked in a national procedure within the scope of EU law. There is a parallel with the rules on data protection. In a procedure before a national supervisory authority under EU data protection law it could be claimed that a data protection right of an individual should be restricted for reasons of national security. Although such a claim may be fully justified, as recognised in Article 13(1)(a) of Directive 95/46, this would not render EU law inapplicable. Declaration (20) attached to the Lisbon Treaty recognises, too, that EU data protection law could have direct implications for national security.

A more thought-provoking issue relates to the applicability of an EU instrument on data protection adopted under Article 16 TFEU693 to national intelligence agencies. Is the consequence of Article 4(2) TEU that any data processing by a national security agency falls outside the scope of Article 16 TFEU, because national security remains the sole responsibility of Member States?

In our view the ruling in ZZ gives an indication that Article 4(2) TEU excludes the competence of the European Union to regulate the activities of the intelligence agencies as such, and for instance to determine their priorities or work methods, but that the same provision does not exclude that general EU standards on fundamental rights or the rule of law are applicable. If this holds true, the data protection regime based on Article 16 TFEU could,

---

689 Case C-300/11, ZZ, EU:C:2013:363, at 66.
690 Case C-300/11, ZZ, EU:C:2013:363, at 38.
691 Pre-Lisbon case law, so before the inclusion of a *national* security exception in the Treaties.
692 E.g., Case C-387/05, Commission v Italy, EU:C:2009:781, at 55.
693 The reference to Article 39 TEU does not apply because a national agency is not part of the Common Foreign and Security Policy.
in principle, be applied to national security agencies. This conclusion does not alter the fact that both the present and the proposed EU instruments exclude state security or national security.\textsuperscript{694}

**National security of third countries**

In the aftermath of the Snowden affair it was argued that the national security exception under Article 4(2) TEU does not apply to the surveillance activities by the NSA, since the exception is connected to the essential state functions of a Member State and thus does not extend to the national security of a third country.\textsuperscript{695} The link in Article 4(2) TEU to the national identity of the Member States justifies the point of view that the national security of third countries is not covered by this exemption from Union competence.\textsuperscript{696} A further argument in support of this view can be found in Schrems.\textsuperscript{697} An essential element in this ruling was the interference with the right to privacy for the objective of national security of the United States. This interference falls within the scope of EU law.

However, the above does not automatically mean that the activities of third countries’ intelligence services are per se not covered by the national security exception under Article 4(2) TEU. For instance, these services of third countries may cooperate with authorities of Member States.\textsuperscript{698} Another possible scenario is that Member States claim that intelligence services of third countries act in the interests of their national security.

Yet, the Snowden affair illustrates that, although fundamental rights have a universal nature, there are areas where the European Union lacks competence to provide effective protection, if only because surveillance activities are also carried out by the intelligence agencies of Member States, sometimes in cooperation with authorities of the United States.\textsuperscript{699}

**Cultural differences and cultural diversity**

\textsuperscript{694} See Article 3(2) of Directive 95/46 (mentioning State security) and Article 2(1) of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final (mentioning national security).


\textsuperscript{696} In this sense also, European Data Protection Supervisor, Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", at 19.

\textsuperscript{697} Case C-362/14, Schrems, EU:C:2015:650, e.g. at 87-88.

\textsuperscript{698} An obvious example is the ‘Five Eyes’ network, an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

The Treaties do not only require respect for national identities, but also for cultural diversity. Under Article 3 TEU, the Union shall respect its rich cultural and linguistic diversity. According to Article 22 Charter the religious diversity shall also be respected. These general requirements are specified in Article 167(4) TFEU: “The Union shall take cultural aspects into account in its action under other provisions of the Treaties, in particular in order to respect and to promote the diversity of its cultures.”

These requirements are significant where privacy and data protection coincides with the freedom of expression and information⁷⁰⁰, and they may also play a role where Member States claim diversity in relation to privacy and data protection itself. An example is the cultural divide within Europe concerning information on income and other revenues. The facts in Satamedia⁷⁰¹ illustrate that in Finland the transparency of these financial data is the rule. At the basis of this case was a newspaper, the main purpose of which was to publish personal tax information. This publication comprised precise information relating to a considerable part of the Finnish residents on their earned and unearned income and the wealth tax levied on them. What is remarkable from a cultural diversity perspective is that the preliminary question posed to the European Court of Justice by the national Finnish judge was not about the transparency of the information as such, nor about the initial publication, but only about further processing of this information. In other parts of the European Union personal tax information is not public and considered to be of a confidential nature.

The need to respect cultural diversity may play a role in the exercise of the mandate of the European Union under Article 16 TFEU and may lead to some leeway being given to cultural differences in the Member States.

### 6. Further Limitations due to the EU’s Organisational Structure: Decentralised Implementation

**Decentralised implementation and cooperation**

Whilst legislation is adopted at EU level, implementation and enforcement mostly take place at national level by national authorities within the national legal systems. As a rule, the European Union is not competent to implement and ensure compliance with its acts.⁷⁰² The Union is not a federal state, but, as Lenaerts & van Nuffel explain, it does exhibit some characteristic features of a federal system, for which they use the term executive

---

⁷⁰⁰ See also Chapter 5, Section 12 and Chapter 6, Section 7 of this study. The freedom of expression and information in Article 11 Charter also includes pluralism of the media. Further read: K. Irion and P. Valcke, “Cultural diversity in the digital age: EU competences, policies and regulations for diverse audiovisual and online content” in: E. Psychogiopoulou (ed.), Cultural Governance and the European Union, Houndmills and New York: Palgrave Macmillan, 2014.


⁷⁰² There are a number of exceptions wherein EU bodies have enforcement powers. An important exception is laid down in Article 105 TFEU, which provides that the Commission shall ensure the application of the principles of EU competition law. Also Article 127(6) TFEU provides that the Council may, by unanimity, confer specific tasks of prudential supervision on the ECB.
In this system the authorities of the Member States must respect the principle of sincere cooperation (Article 4(3) TEU) and the principles of equivalence and effectiveness as developed in the case law of the Court of Justice of the European Union. The exercise of their powers is ultimately under the control of the Court, all with full respect of the fundamental rights as guaranteed by the Charter and the European Convention on Human Rights.

However, despite these safeguards, this decentralised system may complicate effective EU action in the domain of privacy and data protection in an internet environment, where implementation and enforcement has, by its very nature, a cross-border effect and takes place in a technological context where quick responses may often be needed involving actors within various jurisdictions.

In the EU law system, the legislative tasks are generally assigned to the EU level, whereas the executive tasks are vested in the Member States. Under Article 4(3) TEU the Member States “shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.” Authorities of the Member States operate primarily within the national jurisdiction and are subject to review by national courts. The modalities for the exercise of the national authorities’ tasks are determined by their national constitutional systems. However, EU law limits the discretion of the Member States. Two key restrictions are: the principle of sincere cooperation and the responsibility of Member States to protect EU fundamental rights.

**Sincere cooperation as a means to regain control over fundamental rights protection**

The principle of sincere cooperation requires that “the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.” The Court of Justice of the European Union has defined this principle as an expression of solidarity within the system of the Union. The principle is elaborated in obligations for Member States, but the institutions, too, shall practice mutual sincere cooperation. A number of requirements developed on the basis of the principle of sincere cooperation must ensure that Member States give full effect to EU law and that the Member States and the EU institutions cooperate in a fruitful way. The principle of sincere cooperation has specific significance in the context of the Union’s external action, ensuring that Member States do not deviate from positions taken by the Union in negotiations with third countries.

---

704 See on this EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, Chapter 8, and in particular at 220 where the authors speak of “practical possibility” as a species of effectiveness.
706 Article 4(3) TEU.
708 Article 13(2) TEU.
and international organisations. The principle of sincere cooperation is also guiding in the activities of the independent data protection authorities under Article 16 TFEU.

This general principle of sincere cooperation under EU law is specified in a wide range of legislative instruments of the European Union, for specific sectors. Thus, the obligation under Directive 95/46 of the supervisory authorities for data protection to cooperate with one another to the extent necessary for the performance of their duties is a specification of the principle of sincere cooperation.

In the area of this study, which was triggered by the loss of control over personal data on the internet, the principle of sincere cooperation has an additional dimension. Cooperation between the various levels and actors may compensate for the loss of power of individual public entities within a globalised society. Arguably, the loss of control of the European Union and the Member States reinforces the obligations under the principle of sincere cooperation. Complementary action of the various actors in the Union and the Member States is a means to regain control. This view is reflected in debates on multi-level or network governance, or multi-level constitutionalism.

Member States’ responsibility to protect the fundamental rights of privacy and data protection may qualify as a species of sincere cooperation in the context of Article 16 TFEU. In addition, the Member States’ obligation to respect the fundamental rights provided for in the Charter follows directly from Article 51 Charter, as interpreted in Åkerberg Fransson.

In N.S., a case relating to the Common European Asylum System, the European Court of Justice dealt with the Member States’ responsibility to respect fundamental rights when they act within the scope of EU law and the Charter is applicable. The Court confirmed that Member States must make sure that they interpret EU legal instruments in accordance with the fundamental rights of the Union. This means, in addition, that a Member State should not recognise fundamental rights protection in another Member State, when there are substantial grounds for believing that systemic deficiencies in the protection of fundamental rights exist in that other state. In other words, there is a rebuttable presumption that another Member State complies. Where a Member State does systemically not comply with the

---

711 See Chapters 7 and 8 of this study.
712 Article 28(6) of Directive 95/46.
715 Case C-617/10, Åkerberg Fransson, EU:C:2013:280.
716 Joined cases C-411/10 and C-493/10, N.S., and M.E. and Others, EU:C:2011:865.
717 The ruling, at 64, referred to implementing EU law by the Member States under Article 51 Charter, but Åkerberg Fransson gives a wide interpretation to this article 51.
718 At 77 of the ruling.
719 At 86 and 104 of the ruling.
obligation to protect fundamental rights, there may be an obligation of the European Union to guarantee that individuals can invoke their rights.\textsuperscript{720}

More generally, in the system of decentralised implementation, enforcement and judicial protection the European Commission has the task to ensure the application of EU law\textsuperscript{721} and more particularly, to guarantee that Member States and their authorities comply with EU law. The infringement procedure under Article 258 TFEU is an important instrument for the fulfilment of this task.\textsuperscript{722} The European Court of Justice accepts a wide discretion of the Commission in deciding whether or not to instigate proceedings under this provision. The Court examines whether an infringement exists, but does not judge the motives of the Commission for bringing – or not bringing – a case before it.\textsuperscript{723} In the area of data protection, the Commission has not played an active role in bringing infringement cases before the Court, apart from three cases on the independence of data protection authorities.\textsuperscript{724}

7. \textit{Enforcement and the Organisation of Judicial Protection are normally Tasks of the Member States}

Enforcement of EU law is primarily a task of the Member States, albeit under the general conditions of EU law. The Member States must pay due regard to the requirements of uniform application and sanctions must be effective, proportionate and dissuasive.\textsuperscript{725} EU institutions do not operate directly within the territory of the Member States, but through national institutions and authorities.\textsuperscript{726}

The European Union only has the power to enforce directly vis-à-vis private parties in a few specific sectors, the best known being the enforcement of EU competition law by the European Commission.\textsuperscript{727} In this domain, the Commission has powers of investigation in the Member States and may impose penalties.\textsuperscript{728} In addition, outside the area of competition law, a growing number of EU agencies has been given binding decision-making powers vis-à-vis

\begin{footnotesize}
\begin{tabular}{p{1\textwidth}}
\footnote{720}{This argument is made in relation to EU citizenship, in: Armin von Bogdandy, Matthias Kottmann, Carlino Antpöbler, Johanna Dickschen, Simon Hentrei, Maja Smrkolj, “Reverse Solange–Protecting the essence of fundamental rights against EU Member States”, \textit{CMLR} 49, pp. 489–519.}
\footnote{721}{As laid down in Article 17 TFEU.}
\footnote{722}{This procedure was described as an objective method for ensuring Member State compliance of EU law, not a procedure providing individuals with a means of address; see: EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, at 410.}
\footnote{723}{Further read: EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, at 415–418.}
\footnote{726}{In this sense: Carol Harlow, “Three Phases in the Evolution of EU Administrative Law”, in: Paul Craig and Grainne de Búrca, The evolution of EU Law (second edition), (Oxford University Press, 2011), Chapter 15.}
\footnote{727}{Under Articles 101 and 102 TFEU and Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1/1.}
\footnote{728}{Under Chapter V and VI of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1/1.}
\end{tabular}
\end{footnotesize}
private parties. These are however exceptions to the rule that the Member States enforce EU law.

In the area of criminal law this enforcement rule is most evident. The Treaties do not touch upon the Member States’ monopoly of the use of force. The Treaty on the Functioning of the European Union only confers supporting competences on the Union, and where the Treaty provides for operational cooperation, a unanimous Council decision is needed. Also, Europol’s mission is limited to supporting and strengthening action by the Member States’ police authorities.

Administrative law enforcement: multi-level governance or shared administration

In areas of administrative law enforcement the situation is more mixed, also because of the contribution by EU agencies and EU networks, creating multi-level forms of governance, including enforcement. Harlow uses the term “shared administration”.

The provisions on the independent data protection authorities in the proposal for a General Data Protection Regulation are an illustration of the concept of shared administration. These provisions do not only include a cooperation mechanism that is supposed to carry out enforcement tasks in a networked structure within which the EU level and the national level participate, they also precisely circumscribe the tasks of the national supervisory authorities, their discretionary powers as well as the administrative sanctions they must impose in case of breaches of data protection law. These EU provisions apply even when authorities fulfil their tasks within the national jurisdiction without input of the cooperation mechanisms between the authorities. In short, Member States enforce the rules on data protection, but the enforcement is subject to conditions laid down in EU law.

Judicial protection: the principle of national procedural autonomy

The principle of national procedural autonomy or national procedural responsibility is part of the constitutional configuration of the European Union, as developed in the case law

---

729 Further read: EU Agencies in between Institutions and Member States, Edited by: Michelle Everson, Cosimo Monda, Ellen Vos, January 2014. As the title of the book reveals, there is no communis opinio of the place of EU agencies, as part of the EU executive. They are also considered to be hybrid constructions in between the EU and the Member States. See Chapter 7, Section 8 of this study.

730 The Bundesverfassungsgericht underlined this monopoly as a particular sensitive area that should remain with the national state, see Section 8 below.

731 Article 87 TFEU.

732 Article 88 TFEU.

733 Carol Harlow, “Three Phases in the Evolution of EU Administrative Law” in: The evolution of EU Law, Second Edition, Paul Craig and Grainne de Burca, Oxford University Press, 2011, e.g. at 450. See further Chapter 8, Section 7 of this study.


736 Case C-93/12, Agrokonsulting-04, EU:C:2013:432, at 35. See also, Koen Lenaerts, Ignace Maselis and Kathleen Gutman, EU Procedural Law, Oxford University Press, 2014, at 4.01 and 4.02.
of the European Court of Justice. National courts are entrusted with ensuring the legal protection of the citizens under EU law in accordance with the principles of equivalence and practical possibility or effectiveness. Remedies and forms of action must be equivalent to the remedies used to observe national law and the exercise of a right under EU law must be possible in practice. Since the entry into force of the Lisbon Treaty, Article 19 TEU lays down that: “Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law.”

Nevertheless, the principle of national procedural autonomy poses challenges for the effectiveness and uniform application of EU law. There is abundant case law on the balancing between the requirement of effective legal protection on the one hand and national procedural autonomy on the other. This case law has become gradually stricter, leaving less discretion to the Member States. Sometimes EU instruments provide that specific remedies and sanctions need to be made available, of which Chapter VIII of the proposed General Data Protection Regulation is a good example.

This study discusses the national procedural autonomy in particular in relation to the position of the independent data protection authorities and the cooperation between these authorities. An issue is how to ensure the judicial review of actions of these authorities, in particular in cases with cross-border elements.

8. Democratic Legitimacy of EU Action under Article 16 TFEU: A Prerequisite for Trust

This study is based on the presumption that ensuring privacy and data protection on the internet requires trust, also in view of the perceived loss of control over personal data. If the European Union were to regain control, this would benefit both the individuals whose fundamental rights are at stake and the general trust in the Union. In view of this double objective, the effectiveness of the protection (output legitimacy) cannot be sufficient for trust. Democratic legitimacy (or input legitimacy) is also required. The following sections are meant to give context to EU action under Article 16 TFEU and, hence, go beyond the limited understanding of legitimacy given in Chapter 1 of this study.

Considering the main substance of Article 16 TFEU, democratic legitimacy requires specific attention. On the basis of Article 16 TFEU the European Union exercises powers to protect

---

737 This may better reflect the task of the Member States in determining the procedural conditions for ensuring EU law; see: EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, at 220.
738 Starting with Case 33/76, Rehe-Zentralfinanz, EU:C:1976:188.
741 As described in EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, Chapter 8
743 See Chapters 7 and 8 of this study.
fundamental rights of individuals, a subject matter closely related to the traditional state function of ensuring the protection of fundamental rights. Article 16 TFEU leaves little room for the Member States to exercise autonomous powers, it rather leads to an unconditional exercise of powers by the Union, taking precedence over national powers.

Fundamental rights and the academic controversy on democratic legitimacy

A controversy in the academic discussion relating to the democratic legitimacy of the European Union is whether this legitimacy depends mainly on the existence of adequate checks and balances limiting government power and protecting against the tyranny of a majority (or a powerful minority) or whether government power must be based on electoral accountability in order to be legitimate. The absence of the latter link is the most important democratic deficit (of the Union). This is all well described by Craig. On the one hand, there are the views of Monnet representing, roughly, a technocratic vision of democracy defined as neofunctionalist. These views emerge in the approach of Moravcsik, who defends the EU system against the accusations of a democratic deficit. On the other hand, Weiler and others strongly argue against the democratic legitimacy of the Union, precisely because of the absence of accountability in free elections.

In our view, and in line with the views of Weiler and others, it is difficult to deny the importance of the relationship between legitimacy of government action and elections expressing the will of the people. In this regard, reference may be made to Article 21 of the Universal Declaration of Human Rights: “The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.” The EU Charter of Fundamental Rights is more modest in its wording, but nevertheless Article 12(2) Charter reads: “Political parties at Union level contribute to expressing the political will of the citizens of the Union.”

This controversy on the democratic legitimacy of the European Union has wider relevance for this study, especially because it analyses the domain of fundamental rights, which is close to the citizen. Democratic shortcomings of and a lack of support for the Union are matters of concern, also because the use of the wide powers on data protection afforded to the Union under Article 16 TFEU delimits the discretion of democratically legitimised national governments, in connection to fundamental rights protection.

744 As will be further explained in Chapter 6, Section 2 of this study.
745 See on this: P. Popelier, Europe Clauses’ and Constitutional Strategies in the Face of Multi-Level Governance, Maastricht Journal of European and Comparative Law 2014, at 300.
749 Craig submits that not many commentators support the views of Moravcsik.
The legitimacy of EU action depends on the subject area

The German constitutional court made an attempt to classify certain areas of government intervention in its Lisbon ruling,\footnote{2 BvR 2661/06, 6 July 2009, e.g. at 249.} in which it ruled that certain areas are of such a sensitive nature that sufficient room must be left to the Member States\footnote{The list of sensitive areas is also relevant for subjects that would qualify as being part of the national identity (as meant in Article 4(2) TEU). It is wider than the subjects mentioned here. Further read: Armin von Bogdandy, Stephan Schill ‘Overcoming absolute primacy: Respect for national identity under the Lisbon Treaty’, CMLR 48, 2011, Issue 5, pp. 1417–1453, at 1435-1436.} and competences should not be fully transferred to the European Union. The Bundesverfassungsgericht mentioned, in particular, “areas which shape the citizens’ living conditions”. This includes the private sphere of the individual protected by fundamental rights, as well as a variety of cultural issues including the freedom of opinion, press and association. It also mentioned areas which are “particularly sensitive for the ability of a constitutional state to shape itself”, such as the police’s monopoly to use force within the state.\footnote{And – less relevant here – the monopoly of the use of force by the military towards the exterior; at 252 of the ruling. Also, decisions of substantive and formal criminal law are mentioned.} This approach of the German constitutional court has been criticised,\footnote{E.g. in: Daniel Halberstam and Christoph Möllers, The German Constitutional Court says “Ja zu Deutschland!”, 10 German Law Journal 1241-1258 (2009), at 241.} but in essence it is useful for the subject of this study.

The mandate of the European Union under Article 16 TFEU deals with a sensitive area, as explained by the German constitutional court. The fundamental rights of privacy and data protection are essential societal values that deserve protection. This protection also implies the balancing with other fundamental rights. Moreover, in quite a number of situations privacy and data protection require balancing with the protection of physical security, traditionally a state function.

The Lisbon ruling of German constitutional court illustrates that certain elements of the mandate of the European Union under Article 16 TFEU are related to direct interests of individuals and to essential state functions. Payandeh mentions these two aspects as subjects that the Bundesverfassungsgericht claims it may review under EU law.\footnote{The third subject where such a claim is made is ultra vires review, referred to below in Section 13, Mehrdad Payandeh ‘Constitutional review of EU law after Honeywell: Contextualizing the relationship between the German Constitutional Court and the EU Court of Justice’, (2011) 48 CMLR, Issue 1, pp. 9–38.} Although assessing the value of the Lisbon ruling of the German constitutional court falls outside the scope of this study, this ruling supports the argument that for these aspects the input legitimacy plays a strong role.

This is not a plea for a (re)nationalisation of privacy and data protection as long as the democratic legitimacy of the Union is still incomplete. However, the argument does show a paradox. On the one hand, in domains where essential values affecting EU citizens are at stake, these citizens may expect to be effectively protected. The citizens’ trust in an effective and protective government is key in these domains. From the perspective of effectiveness, the European Union is best placed to ensure privacy and data protection in an internet...
environment, also taking into account the principle of subsidiarity. On the other hand, these are politically sensitive domains requiring sensitive policy choices, precisely because of the direct connection with citizens. This is even more obvious where privacy needs to be balanced with security or with the freedom of expression. From the perspective of legitimacy, there should be full democratic control. This requires that government action is subject to high standards of democratic accountability. EU action should thus comply with high standards, both in terms of effectiveness (output legitimacy) and of democratic legitimacy (input legitimacy).  

9. The EU and its Citizens: The Concept of EU Citizenship contributes to the Legitimacy of the EU’s role under Article 16 TFEU

Democratic legitimacy and accountability is an underlying theme that pops up in various chapters of this study, since it is a precondition for restoring trust in governments. Governmental actors need to be democratically legitimised and fully accountable for all their acts. The democratic legitimacy of the European Union is one of the widest debated topics in relation to the Union’s powers and actions. This study does not aim to add new substantial ideas to this debate. The ambition is more modest: understanding legitimacy in order to provide a perspective for EU action under Article 16 TFEU, which justifies EU action and gives insight into its restrictions and limitations.

The first interlocutors of the European Union are – logically speaking – the individuals, in the foundational part of the Treaties, including the Charter, also mentioned as peoples or citizens. Article 1 TEU underlines “the process of creating an ever closer union among the peoples of Europe”. The preamble of the Charter contains the same notion and declares: “[The Union] places the individual at the heart of its activities, by establishing the citizenship of the Union.” Under Article 20(2) TFEU EU citizens shall enjoy the rights and be subject to the duties under the Treaties.

The relation between the Union and individuals has various dimensions, but it is key that individuals may expect effective privacy and data protection under EU law, on the basis of the EU mandate under Article 16 TFEU. As explained, they may also claim that the Union’s intervention is democratically legitimised. Other relevant dimensions are the access individuals should have to justice – or wider, to remedies – under the rule of law, as well as the balancing between privacy and data protection rights and other legitimate interests of.

755 Dougan shows this is not easy, where he explains that the Lisbon Treaty succeeds in terms of effectiveness (“Europe of results”), but not in terms of understanding and acceptance; Michael Dougan, The Treaty of Lisbon 2007: Winning minds, not hearts’ (2008) 45 CMLR, Issue 3, pp. 617–703, at 702.
756 Hereafter simplified to the term of ‘democratic legitimacy’.
757 Without entering into a debate whether the EU primarily unites individuals or Member States; this order is in any event logical in this study since it deals with fundamental rights.
758 Article 20(2) TFEU enumerates a few specific rights of the citizen of the Union, not relevant for his study.
759 Such as remedies before the supervisory authorities for data protection under Article 8(3) Charter and Article 16(2) TFEU.
citizens, be it the exercise of other fundamental rights, the safeguarding of security or other interests.\textsuperscript{760}

An additional observation concerns the scope of EU privacy and data protection \textit{ratione personae}. The Charter applies to all individuals within the scope of EU law, regardless of their nationality or residence. Where the treaties mention the peoples of Europe\textsuperscript{761} this group obviously is narrower, as EU citizens are only those persons having the nationality of a Member State.\textsuperscript{762} This study, dealing with Article 16 TFEU and Articles 7 and 8 of the Charter, normally concerns the widest group ("individuals"), however subject to the following nuance: there is a link between the legitimacy of the European Union as an actor in the protection of fundamental rights on the internet and EU citizenship. EU citizens may, precisely because of their status as EU citizen, expect that the Union effectively protects their fundamental rights to privacy and data protection.

The European Union does not only deal with natural persons, but also with companies and legal persons. Their legitimate interests necessarily play an important role in this study, if only because the first responsibility for ensuring privacy and data protection on the internet lies with those processing personal information, quite often private companies or non-profit organisations. These actors are also expected to cooperate with governmental actors on governance issues. Their role will be addressed in several parts of this study, but not as key interlocutors for privacy and data protection.\textsuperscript{763} The study does not address the complex doctrine on the protection of fundamental rights of legal persons.\textsuperscript{764}

\textit{EU citizenship: EU citizens’ expectations that their rights are protected}

A lot has been written on EU citizenship, in particular in relation to the rights of free movement of EU citizens within the European Union and the prohibition of discrimination on grounds of nationality, as well as on the political rights of EU citizens.\textsuperscript{765} This study does not deal with the specific rights of EU citizens and the limitations of those rights, nor is it focused on EU citizens.

However, EU citizenship is relevant for two – closely interlinked – reasons. Firstly, arguably, EU citizenship gives a title to the legitimate expectation of the citizens that the European Union effectively protects their fundamental rights. Secondly, the aim of fulfilling this

\textsuperscript{760} These dimensions are elaborated in different sections of Chapter 5 of the study.

\textsuperscript{761} See, e.g., the recitals of the TEU: “Desiring to deepen the solidarity between their peoples while respecting their history, their culture and their traditions.”

\textsuperscript{762} EU citizenship is defined in Article 20(1) TFEU: “Every person holding the nationality of a Member State shall be a citizen of the Union. Citizenship of the Union shall be additional to and not replace national citizenship.”

\textsuperscript{763} This choice is justified by the starting point of the study that the protection of fundamental rights – as a public good – is a primary responsibility of government (on different governmental levels).


expectation possibly provides legitimacy to EU action on privacy and data protection. The link between these reasons is that enjoying the right to privacy and data protection, as guaranteed under the specific mandate of Article 16 TFEU, gives substance to EU citizenship.

In *Grzelczyk* the Court of Justice of the European Union defined for the first time the notion of EU citizenship as “destined to be the fundamental status of nationals of the Member States”. The ruling in *Ruiz Zambrano* confirmed that EU citizenship – despite the discussions as to whether or not the Union represents a European demos – is not an empty shell and has substantive meaning. The Court ruled that “Article 20 TFEU precludes national measures which have the effect of depriving citizens of the Union of the genuine enjoyment of the substance of the rights conferred by virtue of their status as citizens of the Union.” Although EU citizenship is closely linked to free movement, a number of rights included in the TFEU for EU citizens are not or not directly related to free movement. Moreover, EU citizenship is widely interpreted and in *Ruiz Zambrano* it also applies to internal, domestic situations extending the rights of the EU citizen to situations where citizens did not move between Member States.

Furthermore, there is a clear, albeit not uncontested link between EU citizenship and the right to invoke fundamental rights. This link is based on the case law of the European Court of Justice, although it is not explicitly confirmed by the Court. Von Bogdandy *et al.* argue that citizenship and fundamental rights are mutually strengthening concepts, having as the same objective bringing the European Union closer to the individual.

These considerations support the argument that there is a relationship between EU citizenship and the specific mandate of the EU under Article 16 TFEU. Article 16 TFEU gives the EU a mandate that must ensure that everyone’s right to data protection is respected. We also recall that effective protection of privacy and data protection cannot be provided by the Member States individually. The exercise of this mandate under Article 16 TFEU contributes to the

---

768 Shaw calls this “the fundamental demos/no demos debate”; see: Jo Shaw in: The evolution of EU Law, Second Edition, Paul Craig and Grainne de Burca, Oxford University Press 2011, Chapter 19, at 582. See also Section 11 of this chapter on social legitimacy.
769 These are the rights to vote, to enjoy diplomatic and consular protection and to petition in Article 20(2)(b), (c) and (d) TFEU.
771 See on this: Armin Von Bogdandy, Matthias Kottmann, Carlino Antpöhler, Johanna Dickschen, Simon Henriët, Maja Smrkolj, *Reverse Solange–Protecting the essence of fundamental rights against EU Member States*, CMLR 49, Issue 2, pp. 489–519, e.g. at 505-506 and the references to opinions of AG Jacobs therein.
772 Armin Von Bogdandy, Matthias Kottmann, Carlino Antpöhler, Johanna Dickschen, Simon Henriët, Maja Smrkolj, *Reverse Solange–Protecting the essence of fundamental rights against EU Member States*, CMLR 49, Issue 2, pp. 489–519, e.g. at 506.
773 In accordance with the principle of subsidiarity, as has been explained in Section 4 above.

142
genuine enjoyment of citizenship of the Union. Therefore, this argument gives legitimacy to the action of the EU under Article 16 TFEU. To avoid misunderstandings, the argument does not exclude third country nationals from protection, nor subjects them to a lower level of protection. They are individuals who are fully protected by Article 16 TFEU and Articles 7 and 8 Charter.

10. Four Arguments Relating to a Lack of Legitimacy of EU Action

Weiler explains that for him the most important constitutional moment in the history of the European Union is not the Schuman Declaration of 1950, nor the Treaty of Rome of 1957, but the Treaty of Maastricht of 1992. The reason Weiler gives is telling. He explains that the Treaty of Maastricht led for the first time to an intense public reaction, whereas before the political class was mostly supportive and the general population conveniently indifferent. From 1992 on, the – supposed lack of – democratic legitimacy became a widely recognised issue, not only in academic but also in more popular circles.

The lack of legitimacy captured in four arguments

The arguments relating to a lack of legitimacy are various. In this section we distinguish four arguments, without pretending to be exhaustive. The first argument is that the EU – and in earlier stages of EU integration the EEC and the EC – has been characterised as a “juristic idea”, as “constitutional law without politics”, a jurisdiction where the European Court of Justice plays a key role in promoting integration, putting itself in a position which in other jurisdictions is taken by legislative and executive powers. The term “judicialisation” of EU law-making is used.

The second argument is that the Union traditionally has strong elements of a technocracy, delegating decision-making powers to technocrats. The Committee of Permanent Representatives (Coreper) and the various configurations of comitology are the most

774 Inspired by: Reverse Solange–Protecting the essence of fundamental rights against EU Member States’, Armin Von Bogdandy, Matthias Kottmann, Carlino Antpöbler, Johanna Dickschen, Simon Hentrei, Maja Smrkolj, CMLR 49, Issue 2, pp. 489–519, e.g. at 507.

775 Views extracted from The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press 1999, at 4, also mentioning some other important moments in EU history. This book predates the Lisbon Treaty of 2009 by 10 years and also predates the Charter being firstly adopted as a non-binding instrument in 2000. The latter two do not change the sense of Weiler’s statement.


778 A somehow condescending way of describing this phenomenon was used in relation to Case C-518/07, Commission v Germany, on the independence of data protection authorities: a “consciously democracy-repudiating expertocracy”. See annotation by Jiří Zemánek, (2012) 49 CMLR, Issue 5, pp. 1755–1768, at 1756.

779 Although Weiler notes that Coreper was created to make it easier for Member States to swallow European decision-making; see: The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press 1999, at 36. This background could also be an
obvious examples of arrangements where civil servants play a key role in decision making. Some theories attributed a decisive role to the European Commission, which has elements of a technocratic body, in the integration process. These theories were especially dominant in the earlier years of the EU (at that time the EEC). A technocratic, elite-led Europe was an explicit idea of Monnet. Sometimes the term ‘governance’ is used in a sense that experts should be enabled to take decisions outside territorial or democratic frameworks. Stakeholder consultation would be enough. Another way of describing this argument is by pointing at the dominance of the executive within the EU structures.

The third argument relates to the European Parliament and the Council. These are, in principle, democratic institutions, also taking into account that the members of the Council are subject to control by national parliaments. However, the limited role of the European Parliament and the veto power of Member States in the Council – where one Member State is able to block decisions supported by large majorities – have long been mentioned as features which contribute to the lack of democratic legitimacy. These shortcomings have, to a certain extent, been addressed in the successive Treaty changes, with the ordinary legislative procedure as set out in Article 294 TFEU as the most obvious result, ensuring both decision-making power of the European Parliament and qualified majority voting in the Council in large areas of EU action. Also, the European Parliament is now entitled to elect the President of the Commission and it exercises a de facto veto power over each individual nominee for


Article 17(7) TEU. It has to be kept in mind that the choice of the European Parliament is limited, since the European Council proposes a candidate. In 2014, a practical way forward enhancing the role of the European Parliament was the choice of the President of the Commission out of the Spitzenkandidaten put forward by the
a post in the Commission. The Lisbon Treaty includes provisions to further enhance the democratic legitimacy, by giving new powers to national parliaments, in addition to the enhanced role of the European Parliament. National parliaments now have the right to be directly informed of various activities of the Commission. Although this right may be rather formal as most information can be found in the public domain, more importantly, it entails that national parliaments have powers to check whether proposed legislative acts comply with the principle of subsidiarity, using what is often referred to as the ‘yellow card’ procedure.

The fourth argument concerns the lack of transparency in the European Union and in particular in the Council. Transparency is considered one of the most critical elements of democratic legitimacy. To a certain extent, the Treaties now deal with this, by emphasising in primary law – for instance in Articles 10(3) and 15(1) TFEU – that the institutions and bodies of the Union must ensure the openness and transparency of the EU policies. The Treaty on the Functioning of the European Union also provides for direct participation of citizens and civil society in EU actions. Furthermore, under the rule of law there is a full system of judicial protection. However, the Union is still perceived as operating with a significant amount of secrecy arrangements and practices. An example of this is the practice in the context of the ordinary legislative procedure where trilogues between the European Parliament, the Council and the Commission play an important role. Trilogue meetings take place behind closed doors with very little public information on the negotiation process. This was a reason for the European Ombudsman to open an own-initiative inquiry.

Democratic legitimacy formally closer to the optimum, but socially not widely accepted

---


790 Protocol (No 1) on the role of National Parliaments in the European Union, annexed to the TEU and TFEU.


793 E.g., in Article 11 TEU.

794 See on this Chapter 2, Section 5 of this study.

795 As explained by Deirdre Curtin, Challenging executive dominance in European democracy. In C. Joerges & C. Glinski (Eds.), The European crisis and the transformation of transnational governance: authoritarian managerialism versus democratic governance (pp. 203–226), Hart Publishing 2014.

796 Raya Kardasheva, Trilogues in the EU legislature, King’s College London, Department of European and International Studies, Research Paper, 30 April 2012.

797 Chapter 10, Section 10 refers to the trilogue concerning the proposed General Data Protection Regulation.

Despite all the measures, aimed at enhancing the democratic legitimacy of the European Union and bringing the Union closer to the democratic optimum, the debate did not end. In the words of Craig: “The problem has been alleviated but not cured by changes made by the Lisbon Treaty.” In short, neither the European Court of Justice nor the Commission can be held (fully) accountable, whereas the roles of the Council and the European Parliament are still imperfect. For obvious reasons, it remains to be seen whether the Council representing national governments will ever be able to qualify as a fully democratic institution, but also about the democratic nature of the European Parliament there is no communis opinio. The Lisbon ruling of the German constitutional court illustrates this: it classifies the European Parliament as a representation of the peoples of the Member States, not of EU citizens, and not based on equality of votes (“one man one vote”).

This leads to a basic distinction in the understanding of democratic legitimacy. It can be understood as a more formal concept, meaning either that a system rests on some democratic foundation or – stronger – that it is based on a directly elected parliament with full powers. In addition, a more social concept of democratic legitimacy is used which refers to the evidence of wide acceptance in society.

One can argue that in the successive Treaty changes and in particular in the Lisbon Treaty – albeit imperfect – solutions were found for issues relating to the formal aspects of democratic legitimacy. However, this does not necessarily diminish what Weiler called the crisis of social legitimacy.

---

798 Further read: Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell, 2010, Chapter 20. An interesting read is the Lisbon ruling of the Bundesverfassungsgericht (2BvR 2661/06, 6 July 2009, at 276-297). It formulated strong arguments against the level of legitimacy of democracy in the EU, and in particular against the democratic control by the European Parliament, emphasising that the European Parliament does not represent European citizens, but the peoples of the Member States.


801 Of course, in a democratic system the highest court should not be held accountable. The observation is related to the supposed role the CJEU played in the European integration process. As to the accountability of the Commission, under Article 234 TFEU the European Parliament can adopt a motion of censure requiring the Commission (as a whole) to resign.

802 Bundesverfassungsgericht Germany, ruling of 30 June 2009, 2 BvE 2008, at 276 et seq.

803 This relates to the discussion between Moravcsik and Weiler c.s. whether electoral accountability is a prerequisite for democratic legitimacy (see Section 8 of this chapter).

804 Wording taken from The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler (Cambridge University Press, 1999), at 80.


806 This does not necessarily mean that these solutions address all concerns. E.g., the German Bundesverfassungsgericht ruled in its ruling on the Lisbon Treaty (30 June 2009, 2 BvE 2008, at 276 et seq.) that control by the European Parliament as such does not result in full democratic legitimacy.

807 The Constitution of Europe, "Do the new clothes have an emperor?" and other essays on European integration, Joseph Weiler, Cambridge University Press 1999, at 84.
11. The Background According to Weiler: The Crisis of Social Legitimacy

Different perspectives, or “different views from the cathedral”, explain this ‘crisis’ of social legitimacy. First, the consecutive Treaty changes attributed tasks of a different nature to the European Union than the original functions of the Union (more precisely the EEC). Besides the perspective of the single market, the Union now also offers its citizens an area of freedom, security and justice without internal frontiers. Article 6 TEU and the Charter also entrusted the Union with general responsibilities on fundamental rights. Second, opposition grew against the incremental way of extending the Union’s powers, sometimes defined as jurisdiction creep, and against what is sometimes felt as an extensive exercise of the Union’s legislative powers. Finally, and most importantly, the ‘crisis’ is caused by what Weiler describes as the absence of a European demos.

Within Europe the principal focus of collective loyalty is not with the Union. Democratic legitimacy is difficult to obtain when the primary loyalty is not with the Union as a whole but with a part of it, usually a Member State. This has become clear in situations where citizens in more prosperous Member States were asked to contribute to the welfare of less prosperous Member States. The resistance within Northern Europe against contributions to the bailout of Greece during the financial crisis is the obvious example.

This loyalty issue also plays a role where the level of fundamental rights protection is at stake. The legislative procedure on the General Data Protection Regulation provides a good example. Various views coming from Germany were founded on the perception that a considerable reinforcement of the level of data protection in the European Union should not adversely affect any specific existing measure of protection in Germany. The absence of a European demos is also relevant in relation to the democratic accountability of data protection authorities and networks of authorities. According to Bignami, informal

---

809 Article 3(2) TEU.
811 A good example is the letter (in Dutch) of the Dutch Minister of Foreign Affairs to the Dutch Parliament of 19 February 2014, Staat van de Europese Unie 2014 (33887). “The Netherlands is convinced that the time of an ‘ever closer union’ in every possible policy area is behind us.”, see: http://www.economist.com/blogs/charlemagne/2013/06/netherlands-and-eu
814 These views are not exclusively German, but were mostly brought forward by German representatives in the Council. See: Update on the General Data Protection Regulation, on http://www.kwm.com/en/de/knowledge/insights/update-on-the-general-data-protection-regulation-20140424.
networks of authorities require, in order to be legitimate, particularly a public that reacts, be it through the press, elections, lobbying or other avenues.

The rejection of the Constitution for Europe in referendums in France and the Netherlands and the low turnout at European Union elections, as well as the fact that EU elections are dominated by national issues, or at least channel eurosceptic sentiments, are examples of the crisis of social legitimacy. The rejection of the Constitution led to the Lisbon Treaty which is in substance quite similar to the Constitution, but without the form, language and symbols of a European Constitution.

Van Middelaar describes the European integration as a quest for visibility with an audience that supports the integration. In short, the European Union is not perceived as an institution of the citizens. European leaders speak in name of the people whereas many people are not aware that their leaders are speaking in their name. Even stronger, the Union may be perceived as interventionist or as a foreign occupational power. Although this study is not about the social legitimacy of the European Union, Article 16 TFEU provides for a wide mandate for the Union in the area of privacy and data protection, with a direct impact on EU citizens. The exercise of this mandate necessarily takes place against the background of shortcomings in social legitimacy, without a – or without a sufficiently – supportive audience and without a – or without a sufficient – perception that people are being represented by the EU institutions.

This background plays its part in justifying the European Union’s role under Article 16 TFEU. One could argue that the shortcomings in social legitimacy plead against a further role of the Union in relation to the fundamental rights of privacy and data protection. This is in line with the reasoning of Menon & Weatherill who argue that the solution for the absence of a European demos does not lie in making the Union more democratic (more “state-like”), but that the solution is competence control.

In our view, the mandate of Article 16 TFEU makes an alternative solution possible, because a legitimate and effective exercise of the mandate of the European Union in an area close to the citizen makes the Union more visible and shows that it is capable of successfully addressing major challenges. A legitimate and effective exercise of the mandate contributes

---

816 One could argue that the European Parliament elections in 2014 were dominated by EU issues in a number of Member States, but with the result that Eurosceptic parties won.
818 Luuk van Middelaar, The Passage to Europe: How a Continent Became a Union, part III.
819 A good example is obviously the preamble of the TEU, where it speaks about continuing the “process of creating an ever closer union among the peoples of Europe”. The ‘closer Union’ is also mentioned in Article 1 TEU.
to the Union’s social legitimacy. Taking the words of Dougan, this solution does not necessarily win the hearts of Europeans, but it may win their minds.822

12. The Legitimacy of EU Action in Relation to the Member States: A Broad Mandate in a Pluralist Legal Context

The Member States are the second category of interlocutors of the European Union, next to the citizens. As explained, the relation between the Union and the Member States is based on the principles of the conferral of competences and the supremacy of EU law. It is further conditioned by the principles of subsidiarity and proportionality and on this basis regulated in more detail in the Treaties and in other instruments of EU law. The pluralist legal context where the Union and the Member States interact is an intensively and continuously debated topic. Concerns of national sovereignty, national identities and cultural differences between the Member States are part of the legal debate.823

Member States’ reticence to enhance EU power

Member States are reluctant to enhance the powers of the European Union, where these powers are closely related to classical state functions.824 This reluctance may be provoked by a lack of willingness amongst large groups in the population to support the Union, described as the crisis of social legitimacy. Against this background, national sovereignty (or in any event claims relating to sovereignty) is an element that plays a role. The current state of EU integration and the lack of support for further integration make it difficult to ensure the full protection of individuals at the level of the Union.

Examples of the reticence of Member States to enhance the power of the European Union can be found in various discussions about the supervision on EU instruments. During the preparation of the proposal for a General Data Protection Regulation, the European Commission considered setting up an EU Data Protection Agency, but dismissed this option on legal grounds,825 and opted for a more decentralised option with a strong coordination role for a European Data Protection Board. However, this role, too, is being challenged in the Council.826

This reticence has a wider background, as is – for instance – illustrated by the developments in the telecommunications sector. After intensive discussion on a European regulator, the supervision in this sector remained with the national regulators. Goodman explains legislative discussions taking place in the 1990s: the European Parliament and the Commission favoured an EU Regulator, but did not achieve their objective, due to resistance from the Member

823 As explained in section 5 above.
824 The exception for national security is a good example.
States, including policy-makers and regulators. Many years later similar arguments were repeated with the result (in 2009) that the supervision remained on the national level, supported by the Body of European Regulators for Electronic Communications (BEREC) with mainly a consultative role.

In general, transferring competences of Member States to the European Union has taken place more completely and more smoothly in areas of economic cooperation – such as the establishment and the functioning of the internal market – than in more sensitive areas, such as the creation of an area of freedom, security and justice. The best illustration of the differences can be found in the current Treaties, in comparing the wide competences of the EU legislator under Article 114 TFEU (internal market) with the EU power in the area of freedom, security and justice. In the latter area the competences are precisely formulated – as is for instance the case for police and judicial cooperation in criminal matters and the exercise of power is subject to specific procedural limitations. The reluctance of Member States in this more sensitive area does not only have to do with shortcomings in the Union’s legitimacy (discussed in the previous section), but also with preferences in keeping national sovereignty. It is remarkable in this context that Article 16 TFEU confers a wide and relatively unlimited power to the Union to regulate the sensitive area of data protection.

A pluralist legal context

There is a scholarly debate about the qualification of the European Union itself. Should it be compared to a federal state, is it an international organisation or an organisation sui generis creating a new legal order, somewhere in between the national and international domains?

This study follows the sui generis option, for pragmatic reasons. On the one hand, entering the highly political discussion on the European Union as a federal state or even as a superstate would divert the attention from the main subject of this study, privacy and data.

---

830 Articles 82-89 TFEU, and in particular Articles 82 and 87.
831 E.g., Article 87(3) TFEU on operational cooperation of the police contains exceptions to the qualified majority voting in the Council and requires unanimity; Articles 82(3) and 83(3) TFEU provide for emergency brakes where a proposed measure could affect fundamental aspects of a Member State’s criminal justice system.
834 In his essay on the transformation of Europe, Weiler points at views of a European Union having “a federal-type structure” (without mentioning the term superstate) which is obviously in contrast with a more supranationalist foundation; see: The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press 1999, at 16.
protection on the internet. On the other hand, qualifying the Union as an international organisation would not do justice to the Union: EU law has direct effect in the national jurisdiction, EU regulations are binding in their entirety and directly applicable in all Member States\textsuperscript{835} and EU law provides a complete system of legal remedies under the rule of law.\textsuperscript{836}

This organisation \textit{sui generis} has as its main characteristic that it creates a pluralist legal context, where both the European Union and the Member States act. This pluralist legal context is sometimes called constitutional pluralism, referring to plural claims to legal and constitutional authority,\textsuperscript{837} based on the premise that there is no strict hierarchical order between the international,\textsuperscript{838} the EU and the national competences. The pluralist legal context is also criticised for this reason.\textsuperscript{839} The legal debate focuses on the constitutionally fundamental question who – which court – has in the end the last word in case different legal orders claim competence. Within the Union this concerns more specifically the question to what extent a hierarchy exists between EU law and national law.

Although this debate exceeds the subject of this study, the underlying issue is relevant for privacy and data protection. At the time of the adoption of the Commission proposal for the General Data Protection Regulation,\textsuperscript{840} judge Masing, a member of the German constitutional court, wrote a newspaper article\textsuperscript{841} in which he criticised the fact that the entry into force of a directly applicable EU regulation dealing with a fundamental right could mean that certain fundamental rights in the German constitution could no longer be applied. Hence, to a certain extent Member States would be deprived of the power to protect the fundamental rights of their nationals.

\textbf{13. Primacy is Potentially in Conflict with the Protection of Fundamental Rights by the Member States}

The relationship between EU law and national law is based on the notion of primacy, or supremacy, of EU law as developed by the Court of Justice of the European Union, for the first time in \textit{Costa v E.N.E.L.} \textsuperscript{842} Primacy is one of the foundations of EU law\textsuperscript{843} and basically a rule of conflict: when an EU rule applies any conflicting national rule should not be applied.\textsuperscript{844} Primacy was confirmed in a declaration annexed to the Lisbon Treaty recalling

\begin{thebibliography}{99}
\setlength\itemsep{0em}
\item \textsuperscript{835} Article 288(2) TFEU.
\item \textsuperscript{836} Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell, 2010, at I-026.
\item \textsuperscript{837} Wording taken from the Introduction of Gráinne de Búrca, J.H.H. Weiler (eds), The Worlds of European Constitutionalism (Contemporary European Politics), Cambridge University Press 2012.
\item \textsuperscript{838} This is discussed in Chapter 9.
\item \textsuperscript{839} E.g., quite strongly by Christiaan Timmermans in The Magic World of Constitutional Pluralism, European Constitutional Law Review / Volume 10 / Issue 02 / September 2014, pp 349–358.
\item \textsuperscript{840} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
\item \textsuperscript{841} Masing, “Ein Abschied von den Grundrechten”, Süddeutsche Zeitung 9 January 2012.
\item \textsuperscript{842} Case C/64, \textit{Costa v E.N.E.L.}, EU:C:1964:66.
\item \textsuperscript{843} Further read: EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, Chapter 9.
\item \textsuperscript{844} The classic case is \textit{Simmenthal}, C-106/77, EU:C:1978:49, at 21: “[…] every national court must, in a case within its jurisdiction, apply Community law in its entirety and protect rights which the latter confers on
\end{thebibliography}
that EU law has primacy over the law of the Member States.\(^{845}\) Primacy and the exclusive competence of the Court of Justice under EU law also played a decisive role in the – negative – opinion of that Court on the accession agreement of the Union to the European Convention of Human Rights.\(^{846}\)

**Different positions taken on the primacy of EU law by national courts**

The notion of primacy of EU law does not necessarily mean that Member States’ jurisdictions accept that EU arrangements always take precedence over national law.\(^{847}\) High courts in several national jurisdictions contest primacy and the Polish and Lithuanian constitutional courts even reject primacy.\(^{848}\) A number of constitutional courts have taken a more moderate approach, the German constitutional court being the most obvious example.

In its *Honeywell* ruling, the German constitutional court\(^{849}\) confirmed earlier case law in which it stated that the primacy of EU law cannot be comprehensive and that – as authors report\(^{850}\) – the Member States remain the ‘Masters of the Treaties’, keeping the last word. It claimed\(^{851}\) that the review of the Treaties cannot be transferred to the EU bodies alone, even where this may lead to an amendment of the Treaties or to an expansion of the scope of EU competences. In exceptional situations where a breach of competences by the European Union is sufficiently qualified, review by the *Bundesverfassungsgericht* can be considered. In short, the German constitutional court confirmed in this ruling that, at the end of the day, when the limits of EU competences are at stake,\(^{852}\) it does have the power to invalidate EU law.\(^{853}\)

The German constitutional court realises that this tension may be unavoidable and offered a cooperative approach for such situations.\(^{854}\) The cooperative approach even allowed the German constitutional court to ask the Court of Justice of the European Union – for the first time – for a preliminary ruling in *Gauweiler and others*, however without relinquishing its own ultimate responsibility. In this view the ruling of the Court of Justice could thus only be

---

\(^{845}\) Declaration 17 Concerning Primacy.


\(^{847}\) This relates to views on legal or constitutional pluralism.


\(^{849}\) Case 2 BvR 2661/06, 6 July 2010, *Honeywell*, at 57.


\(^{851}\) At 57 of the ruling.

\(^{852}\) Or, in other words, where the EU might act *ultra vires*.

\(^{853}\) This answers, for the *Bundesverfassungsgericht*, what Weiler calls “The Decisive Question” on the autonomy of the EU legal order, The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press 1999, Chapter 9.

\(^{854}\) The CJEU should be involved beforehand, in the context of a preliminary procedure under Article 267 TFEU; at 60 of the ruling.
advisory. The opinion of Advocate General Cruz Villalón explains this ambivalence. The Advocate General also proposes that, in the same spirit of cooperation, the Court should give a ruling without referring to this constitutional debate relating to primacy of EU law, which the Court did.

The case law of national courts in a number of other Member States refers to limitations to primacy, consisting in demands that the European Union exercises its powers without infringing certain fundamental principles relating to the essence of the state. Just to mention three examples: in France, the highest courts ranked EU law below the French Constitution. Italian courts do not accept that EU law has primacy over the Italian Constitution. In Spain, too, the constitutional court expressed reservations against the primacy of EU law over the Constitution.

Popelier makes an interesting distinction between two strategies of Member States relating to the incorporation of EU law into their national constitutional systems. The first strategy is what she calls an ‘enabling strategy’ allowing an unconditional transfer of powers to the European Union and an unconditional precedence of EU law over national law. The second is a ‘legitimacy strategy’, concerned with providing legitimacy to EU law in the national jurisdiction and thus contesting unconditional primacy. The positions of the constitutional courts mentioned above reflect the second strategy.

Some scholars argue that Article 4(2) TEU, insofar as it lays down that the European Union shall respect national identity, nuances the notion of primacy of EU law. Other scholars argue that Article 4(2) does not limit primacy, but must be regarded as a restriction, under EU law itself, to the exercise of EU competences. In this latter view, Article 4(2) TEU does not limit primacy, but the powers conferred on the Union. Advocate General Poiares Maduro expresses an interesting view in Arcelor, a case predating the Lisbon Treaty. He states that the Treaty on European Union itself reassures the Member States that EU law will not threaten national constitutional values, but that the task to protect these values is transferred to the European Court of Justice.

863 Opinion of AG Poiares Maduro in Case C-127/07, Arcelor, at 16.
864 And, thus, based on Article 6 TEU as it was formulated before Lisbon, also including a reference to national values.
In short, there are different views on the role of the European Union and its relation to the Member States. These differences in views can be found amongst the highest courts, as was just illustrated, and also amongst learned scholars. At the centre of this debate stands the qualification of the relationship between the Union and the Member States as heterarchical or as hierarchical, based on supremacy in the areas where EU law applies.  

The concept of primacy and the supposedly hierarchical nature of the EU system are at the heart of the criticism expressed by judge Masing of the German constitutional court in relation to the proposed General Data Protection Regulation. Primacy of EU law means for instance that – particularly after the adoption of the General Data Protection Regulation – EU law does not only impact the possibilities to protect, within the national jurisdiction, the fundamental right to data protection, but also the rights coinciding with it, such as the freedom of expression, where there is an interface with data protection. The scholarly debate therefore has direct impact on the meaning of Article 16 TFEU.

Schrems as example of a potential conflict between primacy and respect of privacy and data protection

The ruling of the European Court of Justice in Schrems revealed a potential conflict between primacy of EU law and ensuring privacy and data protection by authorities of the Member States. This conflict concerns more particularly the duty of these authorities to apply a decision by the European Commission (i.e. the Safe Harbour Decision of 2000), on the one hand, and the power to protect the fundamental rights of individuals who lodged complaints, on the other hand. If the DPAs were to investigate the adequacy of privacy and data protection of in casu the United States, as challenged by the complainant, they would disregard a decision under EU law – the Safe Harbour Decision, which declared that the level of protection was sufficient. This is the essence of the conflict, although the facts in the case were more complicated, since the power of the national data protection authorities (DPAs) to investigate on the basis of a complaint also resulted from EU law. In this particular context, it is irrelevant that the Court’s ruling declared the Safe Harbour Decision invalid.

This conflict of legal obligations – stemming from the notion of primacy – prompted the Court of Justice to a creative solution, requiring the DPA to examine the complaint with due diligence. Due diligence means that in case the DPA considered the complaint well-

---


868 Case C-362/14, Schrems, EU:C:2015:650, at 63.
founded, it could not decide the case itself, but would have to bring the case before a national court which, in turn, could pose preliminary questions to the Court of Justice.

14. **Legitimacy based on Output: Required to regain Control over Privacy and Data Protection, but not Sufficient**

The European Union also acquires legitimacy where it is capable to act in an efficient and effective manner (output legitimacy). Citizens may expect that governments – including the European Union – are able to achieve their tasks effectively. The Snowden affair, one of the triggers for this study, showed that the Union and the Member States were not capable of fulfilling their task in a satisfactory way. In addition, the phenomenon of big data as such implies a lack of control.

Output legitimacy is essential for all government intervention. This is even more significant in the case of international organisations, because an inherent element of those organisations is that their institutions and bodies are not fully accountable for their acts in elections, or because interinstitutional checks and balances are flawed. Obviously, the situation of the European Union in terms of democratic legitimacy is fundamentally different from other international organisations, if only because it has a directly elected European Parliament, even though, as we have seen above, the situation is not yet optimal despite Treaty changes. More specifically, output legitimacy is one of the main reasons justifying intervention by the Union, which is even illustrated by the wording of the principle of subsidiarity in Article 5(3) TEU according to which the EU may act where objectives, by reason of the scale or effects of the proposed action, can be better achieved at Union level.

Menon & Weatherill developed a theory emphasising the dominance of output legitimacy for EU policies and legislation; legitimacy can exist even where input legitimacy is lacking. They basically deny that, on the EU level, a genuine debate on a policy issue can take place giving social legitimacy to the Union as a majoritarian system, with office holders accountable in elections. They explain that precisely because of the independence of institutions like the European Commission – and the absence of input legitimacy – certain interests can be promoted and optimal regulatory decisions can be taken. The authors mention Pareto optimality: the making of markets, for instance, is a technocratic activity aiming at the

---

870 See Chapter 3.
872 This is the criterion for democratic legitimacy in the theory of Moravcsik.
creation of a stable, long term and predictable future for economic actors and should not be constrained by effects of democratic politics.875

Their theory did not receive general support in the legal literature, but contains elements relevant for this study. Menon & Weatherill build their theory on two arguments. First, one should not use state paradigms as starting point for measuring the legitimacy of the European Union, because the Union has tasks that are not state-like, such as eliminating barriers to cross-border trade. Second, states themselves fail to live up to their claims on legitimacy, since also many state policies are not exposed to full democracy.876 Furthermore, EU policies serve as a corrective to imperfect national political processes, for instance since national processes cannot control processes taking place outside their territory.877 Menon & Weatherill conclude that international organisations do not only contribute to efficiency gains, but also compensate for outmoded or unrepresentative political processes.

The dominance of output legitimacy is in particular justified in policy sectors which are efficiency oriented, attempting to increase the aggregate welfare of society,878 for instance by regulating markets, where policy choices can be extracted from majoritarian rule. This is why Menon & Weatherill connect their theory to what they call the “competence control” of the European Union.879 Their theory would not work in policy areas where interests of individuals are at stake.

Craig’s criticism880 on this theory links to this last point. The European Union needs input legitimacy, because it has political authority over a wide range of areas, including the area of freedom, security and justice. Moreover, also the regulation of markets is not necessarily apolitical and therefore also in that area output legitimacy may not be sufficient.881 Furthermore, according to Craig, a theory based on dominance of output legitimacy could also have the undesirable effect that a lack of democracy would sometimes be preferred for reasons of effectiveness. For example, in the past, the European Union also has been effective precisely thanks to a lack of democracy. Illustrations relevant for privacy and data protection are the legislative instruments dealing with the use of personal data adopted by the Council in

876 They give some examples of areas where more or less technocratic instruments prevail at the national level as well, such as competition law or banking policies.
881 Craig points in this context, e.g., to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, at 36), the adoption of which provoked wide reactions in the Member States, e.g. because it would allegedly lead to competition between workers in different parts of Europe – hence the expression “Polish plumber” – resulting in social dumping (source: Wikipedia; see: https://en.wikipedia.org/wiki/Polish_Plumber).
the areas of police and judicial cooperation in criminal matters shortly before the entry into force of the Lisbon Treaty. The Council managed to adopt these legislative instruments shortly before the European Parliament got co-decisive power in this area.\textsuperscript{882} By doing so, the Council gave preference to effective decision-making over democratic support.

A more complex legislative procedure with full competence of the European Parliament and even with procedural guarantees for national parliaments enhances the democratic level of the European Union, but could also prejudice the output legitimacy.\textsuperscript{883} In other words, introducing democratic checks and balances in the decision-making process of the Union could render the Union less effective and consequently diminish the support for EU action. Obviously, this is a reasoning which should not be pursued – the same arguments could apply to each democracy – but it shows the difficulty of EU action where output legitimacy is a big factor of success.\textsuperscript{884}

This being said, in the area of privacy and data protection, output legitimacy is required to regain control over privacy and data protection on the internet, but it is not sufficient due to the nature of the subject matter. Output efficiency requires high standards of effectiveness in view of the phenomena on internet that challenge privacy and data protection. Considerations of legitimacy may limit what would in theory be the most effective outcome.

\textbf{15. Effectiveness: Delivering Privacy on the Ground}

In this study, effectiveness means ensuring that the general principles of privacy and data protection are translated into protection of the individual in practice.\textsuperscript{885} In other words, effectiveness ensures bridging the gap between principles and practice and delivering privacy and data protection in the books as well as on the ground.\textsuperscript{886} Although effectiveness is a different requirement than legitimacy, the two notions are closely linked. As explained, considerations of effectiveness are a constitutive element of legitimacy (output legitimacy).

The analysis of effectiveness starts by recalling that effective application of the law is one of the permanent, invariable notions in the case law of the Court of Justice of the European Union\textsuperscript{887} and a prerequisite for all action within the scope of EU law. Under the Court’s case


\textsuperscript{883} Cassese mentions as a paradox the unavoidable compromises in the EU rendering the EU ineffective, in: Stefano Micossi, Gian Luigi Tosato, Europe in the 21st Century: Perspectives from the Lisbon Treaty, CEPS Studies, 2009, at 3.


\textsuperscript{885} As explained in Chapter 1, Section 1 of this study.


\textsuperscript{887} Mayr explains that the English versions of the Court’s rulings sometimes contain the term ‘effet utile’, but also ‘effectiveness’ or ‘full effectiveness’, more rarely also ‘full force and effect’ or ‘practical effect’; see:
law, the principle of effectiveness encompasses the effective judicial protection of individuals, the need for Member States to uphold the primacy of EU law vis-à-vis national law and the effectiveness of procedures and sanctions.888

Under Article 16 TFEU the European Union has the competence to ensure privacy and data protection. As explained, this is a competence the Union shares with the Member States, but not with the private sector. The effectiveness of protecting the rights laid down in Article 16(1) TFEU and in Articles 7 and 8 Charter is an imperative under EU law. EU law should ensure that these rights are respected, also in horizontal relations between private actors. This imperative must result in a level of protection that fulfils the requirement of effectiveness.889 Effective protection is the way to regain control over privacy and data protection on the internet, as this study explains.890

Effectiveness relates to governance. Hooghe and Marks developed a theory in which they distinguish two types of governance: Type I Governance is defined as federalism and under Type II Governance the citizen is not served by the government but by “a variety of different public service industries”.891 Article 16 TFEU is an exponent of Type I Governance, leaving final responsibility with governmental actors. However, the involvement of various actors including the private sector in the implementation is a component of the governance under Article 16 TFEU, as will be illustrated below. This is also the focus of the reform of the EU rules for data protection. The reform places emphasis on empowerment of the individual, on enhancing the responsibility of the data controllers and, linked to this, on encouraging self-regulatory initiatives and exploring EU certification schemes, as well as on strengthening the position of the independent data protection authorities and their cooperation.892

The following chapters of the study will elaborate how the principle of effectiveness is best observed by the European Union when exercising its three tasks in the area of data protection, i.e. through judicial control by the European Court of Justice, legislation under Article 16(2) TFEU and control by the independent data protection authorities. Effectiveness will also be an element of the substance matter of Chapter 9 on EU action in relation to third countries and international organisations. This section introduces starting points of a more horizontal nature.

**Empowerment of individuals**

889 As a general requirement of EU law; see: EU Law, Text, Cases and Material, Fifth Edition, Paul Craig and Grainne de Burca, 2011, at 223-231.
890 See Chapter 2 of this study.
891 Liesbet Hooghe and Gary Marks, Unraveling the Central State, but How? Types of Multi-level Governance, American Political Science Review Vol. 97, No. 2 May 2003, at 237.
892 E.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final.
Legal instruments must ensure that individuals are able to effectively protect themselves, be in control. As the Commission explains, individuals have the right to enjoy effective control over their personal data.\textsuperscript{893} Control over personal data is in particular challenged in the global and – from the perspective of individuals – technologically complicated information society. This has been one of the triggers for this study. Being in control starts with transparency.\textsuperscript{894} One of the objectives of the data protection reform is “reinforcing the right to information so that individuals fully understand how their personal data is handled”.\textsuperscript{895}

Subsequently, the individual must have the necessary tools to act and to defend his or her rights. The right to be forgotten and to erasure, as interpreted by the Court of Justice of the European Union in \textit{Google Spain} in relation to Directive 95/46\textsuperscript{896} and as more prominently included in the proposed General Data Protection Regulation\textsuperscript{897} is meant for this purpose. It is interesting that Google actually gives effect to this ruling in a way that it empowers individuals to have their information removed. It provides a form for a search removal request and assesses each request individually, which requires balancing this request against the right of the general public to know.\textsuperscript{898} In roughly the first year after the ruling Google has received more than 291,000 requests from individuals.\textsuperscript{899}

The final element of individual control is effective access to remedies under the rule of law, as is also required under Article 13 ECHR and Article 47 Charter. Effective access must be guaranteed for the individuals whose personal data are processed, for parties that process data and for third parties that are directly and individually concerned.\textsuperscript{900} Collective redress mechanisms can be helpful in empowering groups of citizens to combine their claims. The proposed General Data Protection Regulation contains some new elements in this respect. Organisations are entitled to lodge claims with the independent data protection authority and have rights to a judicial remedy, both on behalf of the data subject.\textsuperscript{901}

\textsuperscript{894} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM (2012) 9 final, at 6, also mentions ‘consent’ as an element of control.
\textsuperscript{896} Case C-131/12, \textit{Google Spain and Google Inc.}, EU:C:2014:317, at 96 \textit{et seq.}, where reference is made to Articles 12(b) and 14 of Directive 95/46.
\textsuperscript{898} Available on: https://support.google.com/legal/contact/lr_eudpa?product=websearch.
\textsuperscript{900} Terminology of Article 263(4) TFEU.
\textsuperscript{901} Articles 73 and 76 of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. For amendments to this text, see the European Data Protection Supervisor’s Opinion of 27 July 2015 – Europe’s big opportunity, EDPS recommendations on the EU’s options for data protection reform + Annex - Comparative table of GDPR texts with EDPS recommendations.
Data controllers’ responsibility: multi-stakeholder solutions as an alternative for command-and-control legislation

Enhancing the responsibility of the data controllers, encouraging self-regulatory initiatives and exploring EU certification schemes are objectives of the data protection reform and also play a role in other policy debates. Instruments that are considered for privacy and data protection include multi-stakeholder solutions, where governments work together with representatives of the private sector and of citizens with the aim of developing mechanisms of self-regulation or co-regulation, result-oriented accountability (where the addressee of the law is required to ensure and demonstrate compliance but is free in choosing the means), and standardisation and certification.

Under Article 16 TFEU it must be ensured that addressees of the law – for instance companies operating on the internet, non-profit organisations and public authorities – translate the in themselves abstract requirements of protection of fundamental rights into their daily business practices. The law should give them the right incentives to comply with the law and to effectively protect fundamental rights. These incentives primarily come from governments, using a right mix of legislative and non-legislative tools, but it makes sense to also profit from market forces.

To make it more concrete, governments are in need of alternative angles to traditional command-and-control legislation, in order to effectively intervene in global and technological complex environments. The need for alternative angles to traditional command-and-control legislation is widely recognised and various efforts have taken place under the umbrella of ‘Smart Regulation’. Although the European Commission uses this term mostly in its policies to reduce red tape, under the umbrella of ‘regulatory fitness’, the term is wider, since it refers more in general to smart ways to regulate.

The Juncker Commission considers better regulation as one of its core tasks, which has led to the appointment of first vice-president Timmermans coordinating this area within the Commission. Better regulation includes – as far as relevant for this study – ensuring that EU proposals comply with the principles of subsidiarity and proportionality, removing unnecessary ‘red tape’ and ensuring the quality of impact assessments. The Commission

902 See, e.g., Chapter 6, Section 14, dealing with accountability of controllers and processors of personal data.

903 This is a method which is much relied upon in the US for consumer privacy, White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012 (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).

904 This is an important element of the proposed General Data Protection Regulation (Article 22), although the Commission Proposal for a General Data Protection Regulation uses the term accountability only in the explanatory memorandum. See also the EDPS Opinion of 7 March 2012 on the data protection reform package, at II.6.a.

905 This all will be further developed in Chapter 6 of this study.


907 According to the mission letter of 10 September 2014: “Coordinating the work on better regulation within the Commission, ensuring the compliance of EU proposals with the principles of subsidiarity and proportionality, and working with the European Parliament and the Council to remove unnecessary ‘red tape’ at both European and national level. This includes steering the Commission’s work on the ‘Regulatory Fitness and Performance
adopted a Communication on better regulation\textsuperscript{908} and Better regulation guidelines,\textsuperscript{909} emphasising the need for better regulatory tools. As an element of the Better regulation guidelines the Commission points at the need for considering various policy options, including “Alternative policy instruments: e.g. non-regulatory alternatives; self- or co-regulation; market-based solutions, regulatory alternatives; international standards, and their mix.”\textsuperscript{910}

**Enforcement as a key element of effectiveness**

Effective enforcement mechanisms are indispensable to ensure that the fundamental rights of privacy and data protection are effectively protected. Emphasis on enforcement is even more relevant in a context of a global internet and an evolving era of big data which complicates the tasks of governments to ensure effective protection of constitutional values. Under Article 16 TFEU enforcement entails a key role for the data protection authorities and control by the authorities is even qualified as “an essential component of the protection”.\textsuperscript{911}

As we recalled before, strengthening the position of the independent data protection authorities and their cooperation was an important driver behind the data protection reform.\textsuperscript{912} Appropriate enforcement structures are a prerequisite under the principle of effectiveness.\textsuperscript{913} This is wider than enhancing the role of the data protection authorities. Enforcement of fundamental rights is a responsibility of governments, be it national or EU, in a democratic society and under the rule of law. This does not exclude involvement of other actors, as long as this responsibility is sufficiently ensured.\textsuperscript{914}

Effective enforcement is only possible if the government in its role as legislator – and/or by using non-legislative instruments – provides for the necessary conditions. This means in the first place the right choice of legislative and non-legislative instruments. Effective enforcement should ensure control over personal data. Organisations processing personal data should know what they have to do to protect these fundamental rights and should be given the

\textsuperscript{908} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation for better results - An EU agenda, COM(2015) 215 final
\textsuperscript{911} Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, as recently confirmed in Case C-362/14, Schrems, EU:C:2015:650, at 42. See Chapter 7, Sections 1 and 2 of this study.
\textsuperscript{912} E.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final.
\textsuperscript{913} The role of the data protection authorities and their cooperation is the subject of Chapters 7 and 8.
\textsuperscript{914} Through what is called ‘multi-level governance’, governing by various governmental and non-governmental stakeholders; see: the special issue on Multi-Level Governance, Maastricht Journal of European and Comparative Law 2014/2.
right incentives to protect, individuals should be given the right tools to protect themselves and the data protection authorities should be sufficiently empowered to play their role.  

16. Conclusions

The task of the European Union under Article 16 TFEU is exercised in the sensitive area of fundamental rights, close to the citizen. It is widely formulated, as an obligation of the Union to ensure full protection, thus under Article 16 TFEU data protection is a competence of the Union, leaving very limited discretion for the Member States, particularly after the entry into force of the General Data Protection Regulation, which aims at creating a level playing field in the Union. Article 16 TFEU gives a mandate to the European Union, but the Member States remain important actors.

Legitimacy and effectiveness add new perspectives to the complicated reality of privacy and data protection on the internet. Although different issues, legitimacy and effectiveness are interlinked: legitimacy can be measured in terms of effectiveness, coined as ‘output legitimacy’, as opposed to ‘input legitimacy’, the democratic legitimacy of government action. In a pluralist legal context the European Union takes account of the legitimate interests of individuals and Member States. (Section 2)

Article 16 TFEU confers a broad competence to the European Union, beyond its role in respect of most other fundamental rights. Article 16 TFEU means that privacy and data protection fall by definition within the scope of EU law. Data protection has become a concern of the Union, although the implementation is shared with the Member States. (Section 3)

The exercise of the mandate under Article 16 TFEU should comply with the principles of subsidiarity and proportionality. As a rule, these obligations are fulfilled since efficient and effective privacy and data protection on the internet cannot be sufficiently achieved by the Member States. The study’s position in the debate whether the protection in the public sector – in the light of the subsidiarity principle – should be left to the Member States, is that this should not be the case: there should be no distinction in law between the private and the public sector. The individual deserves equal protection under EU law in the public and the private sectors. (Section 4)

The European Union should respect national identities, national security and cultural differences. The exception of the scope of EU law for national security does not mean that a justified claim based on national security under Article 13 of Directive 95/46 renders EU law inapplicable. The ruling of the European Court of Justice in ZZ gives an argument in support of the application of general EU data protection law to national security services. The ruling in Schrems illustrates that the exception of the scope of EU law does not extend to

---

intelligence services of third countries. The need to respect cultural diversity gives Member States some leeway. (Section 5)

The decentralised implementation of EU law is a further limitation the European Union has to consider in exercising its mandate under Article 16 TFEU. Decentralised implementation requires cooperation between the various actors, under the principle of sincere cooperation. This principle has increased importance in view of the loss of control over personal data on the internet. Cooperation between the various levels and actors could compensate for the loss of power of – individual – public entities within a globalised society. (Section 6)

Under EU law, enforcement and the organisation of the judicial protection are normally tasks of the Member States. The judicial protection is determined by the principle of national procedural autonomy. The provisions on the DPAs in the proposal for a General Data Protection Regulation are an illustration of a shared administration. These provisions precisely prescribe the tasks of the national supervisory authorities, their discretionary powers as well as the administrative sanctions they must impose in case of breaches of data protection law. (Section 7)

Democratic legitimacy of EU action under Article 16 TFEU is a prerequisite for trust, particularly in the domain of privacy and data protection, which is closely related to the traditional state function belonging to the core of a democracy under the rule of law. Data protection is a sensitive area, as confirmed in the Lisbon ruling by the German constitutional court, classifying areas of government intervention. EU action should thus comply with high standards, in terms of legitimacy as well as effectiveness. (Section 8)

The concept of EU citizenship contributes to the legitimacy of the Union’s role under Article 16 TFEU. EU citizenship justifies the expectations of EU citizens that their rights are protected. The exercise of the mandate under Article 16 TFEU contributes to the genuine enjoyment of citizenship of the European Union. Vice versa, this contribution to the enjoyment of citizenship gives legitimacy to the exercise of the EU mandate under Article 16 TFEU. (Section 9)

The study gives four arguments relating to a lack of legitimacy of EU action, in a more general sense. The European Union is a ‘juristic idea’ with its Court of Justice in the position of legislative and executive powers; the Union is a technocracy; the European Parliament and the Council are in principle democratic institutions but with shortcomings; and there is a lack of transparency in the institutions. As a result of the changes to the Treaties solutions, albeit imperfect, were found for issues relating to the more formal aspects of democratic legitimacy, but these changes did not have effect on the “crisis of social legitimacy”, as Weiler puts it. (Section 10)

According to Weiler, the crisis of social legitimacy is caused by the absence of a European demos. The European Union is not perceived as an institution of the citizens. European leaders speak in name of the people whereas many people are not aware that leaders speak in their name. This study claims that a legitimate and effective exercise of the Union’s mandate
under Article 16 TFEU, an area close to the citizens, makes the Union more visible and shows that it is capable to successfully address major challenges. This contributes to the Union’s social legitimacy. (Section 11)

EU action should also be legitimate vis-à-vis the Member States. The European Union and the Member States interact in a pluralist legal context, with plural claims to legal and constitutional authority. Article 16 TFEU confers a broad and relatively unlimited power to the Union to regulate the sensitive area of data protection. This could mean that to a certain extent Member States would be deprived of the power to protect the fundamental rights of their nationals. (Section 12)

Primacy (or supremacy) of EU law is basically a rule of conflict. When an EU rule applies any conflicting national rule should not be applied. Particularly after the adoption of the proposed General Data Protection Regulation, primacy of EU law does, for instance, not only restrict the possibilities to protect the fundamental right to data protection within the national jurisdiction, but also has an impact on the protection on the national level of the rights coinciding with it, such as the freedom of expression. The Court of Justice’s ruling in Schrems revealed a potential conflict between primacy of EU law and ensuring privacy and data protection by Member State authorities. (Section 13)

Citizens may expect that the European Union is able to achieve its tasks effectively, as illustrated by the Snowden revelations (output legitimacy). Output legitimacy is required to regain control over privacy and data protection on the internet. It requires high standards of effectiveness in view of the phenomena on the internet that challenge privacy and data protection. Output efficiency is not sufficient, due to the nature of the subject matter. Considerations of legitimacy may limit what would in theory be the most effective outcome. (Section 14)

Effectiveness means bridging the gap between principles and practice. Involvement of various stakeholders, including the private sector, in the implementation is a component of the governance under Article 16 TFEU. However, the final responsibility stays with governmental actors. Effective governance requires empowerment of the individual, giving responsibility to the data controllers with multi-stakeholder solutions as an alternative for command-and-control legislation, and strong enforcement mechanisms. (Section 15)

This chapter outlined the mandate under Article 16 TFEU. The contributions of the three main actors and roles (the Court of Justice, the EU legislator, the supervisory authorities and their cooperation mechanisms, and the EU as an actor in the external domain) should result in a legitimate and effective structure of EU privacy and data protection. However, the contributions are delivered in a separate manner. In view of the separation of powers, the institutional balance within the European Union and the independence of the data protection authorities, the actors do not work together, but their contributions should be mutually strengthening data protection, in a system of checks and balances.
Chapter 5. Understanding and Assessing the Contribution of the CJEU to the Mandate under Article 16 TFEU

1. Introduction

The European Union has an active obligation to ensure everyone’s rights to privacy and data protection and is responsible for the result. The Court of Justice of the European Union is an important player in ensuring that this obligation is fulfilled.

This chapter analyses the contribution of the EU Court of Justice to the fulfilment of the mandate under Article 16 TFEU. This analysis is a specification of an element of the research question: “what does and should the European Union do to make Article 16 TFEU work, through the judicial review by the Court of Justice?” This analysis includes the following subjects:

- a. the general design of the mandate;
- b. the institutional position of the EU Court of Justice in the constitutional order of the Union and its role as a constitutional court in relation to the protection of fundamental rights;
- c. the Court’s mode of fundamental rights protection, focusing on the emergence of the protection, the nature of the rights and distinctions between rights;
- d. the balancing of privacy and data protection with other fundamental rights and public interests, with a short look at the US Supreme Court;
- e. the balancing focus: the freedom of expression, the right of access to documents, the right to property, including intellectual property, and the public interest of security;
- f. the Court’s contribution under Article 16 TFEU, related to other EU issues.

Examining these subjects has the objectives of gaining an understanding of and further clarifying the contribution of the Court of Justice of the European Union in order to specify what its role should ideally be. This assessment will result in more focus in the conclusions of this chapter, where the following three elements will be emphasised. First, the role of the Court has gradually emerged and gained importance, which it assumes as a means to regain trust in the handling of personal data by a strict review of privacy and data protection, taking the internet context into account. Second, an important task for the Court is to balance privacy and data protection with other fundamental rights. This chapter provides suggestions to distinguish between (categories of) fundamental rights. Third, the Court has clarified a number of issues that are important for protecting privacy and data protection under Article 16 TFEU, whereas other issues require further clarification.

Section 2 gives a general description of the task of the European Court of Justice under Article 16 TFEU and of how to approach the remarkable features of this provision. Sections 3 and 4 discuss the institutional role of the Court in the constitutional order of the European Union. The Court acts as a constitutional court wherever it protects the fundamental rights of
privacy and data protection. Section 4 also considers the Court’s legitimacy and the possibility for the Court to compensate for the democratic deficit of the Union.

Sections 5-9 deal with the fundamental rights protection by the Court of Justice, starting with the emergence of fundamental rights in the EU legal order. The Lisbon Treaty marks the start of a new era reinforcing the role of fundamental rights in the reasoning of the Court. Sections 8 and 9 introduce the substance of fundamental rights, in order to understand the nature of the rights and the differences between fundamental rights. A simple taxonomy is proposed to make distinctions between fundamental rights in an internet context, allowing for a more meaningful balancing between rights and allowing for a concentration of efforts – also in the external domain – on the protection of those rights that are most challenged on the internet.

An important component of the contribution of the Court of Justice to Article 16 TFEU consists in balancing privacy and data protection with other fundamental rights and public interests. This balancing has become more important since on the internet the connection between privacy and data protection and other fundamental rights and public interests has intensified. Section 10 introduces the way in which the Court conducts this balancing of rights and interests, whilst Section 11 gives further context by discussing the US Supreme Court’s approach. Sections 12-17 analyse in greater detail how the Court of Justice balances. Privacy and data protection are balanced with the freedom of expression and information, with the right of access to documents, with the right to property, including intellectual property, and the public interest of security.

The Court of Justice of the European Union also promotes market integration and acts as an umpire where other public interests or other governmental actors have an impact on the exercise of powers under Article 16 TFEU (Section 18). The Court plays its role in order to ensure that the Union’s commitment to ensure privacy and data protection can be realised, but also as an umpire where conflicts of competence arise between the EU and the national level. Section 19 contains the conclusions.

2. The General Design on The Task of the CJEU under Article 16 TFEU: How to cope with the Remarkable Features of this Provision?

Article 16(1) TFEU reads: “Everyone has the right to the protection of personal data concerning them.”

This provision is closely related to Articles 7 and – this is evident – Article 8 of the Charter of the Fundamental Rights of the Union, on the respect of privacy respectively data protection. As has been explained in Chapter 4, Article 16(1) TFEU adds value to these articles in the Charter. Article 16 TFEU establishes a mandate of the European Union in relation to data protection and, by doing so, brings privacy and data protection by definition within the scope of EU law (whereas the scope of the Charter is delimited in Article 51(2) thereof). Article 16 TFEU confirms the active obligation for the Union to ensure protection.
Chapter 2 discussed the substantive content of privacy and data protection as fundamental rights that matter in an information society: they are essential in a European Union based on values. It also defined privacy and data protection as inextricably linked. Data protection was described as the right of an individual for his data to be processed in a fair manner, thereby reinforcing the underlying value of privacy. The chapter regarded privacy and data protection as two sides of the same coin; privacy represents the value and data protection determines the rules of the game. This justifies these two rights being protected in an integrated manner.

As Chapter 3 explained, the features of the internet and the development of communications on the internet have caused a loss of control of European governments and EU institutions. These features and developments reinforce the positive obligation to protect individuals, also in horizontal situations where private parties process personal data. It is not claimed, however, that privacy and data protection are absolute rights and, therefore, limitations and restrictions are needed.

This all defines the Court of Justice’s contribution, which by definition primarily affects individuals, the first category of interlocutors of the European Union as described in Chapter 4. Article 16(1) TFEU does indeed grant a right to individuals.

The Court of Justice of the European Union should, in the first place, further clarify Article 16 TFEU. Leaving aside its substantive content, Article 16(1) TFEU has remarkable features. To begin with, it establishes a right, but does not specify its content. The main elements of the substance of the right laid down in Article 16(1) TFEU are included in Article 8(2) Charter. Further elements are included in secondary law, with Directive 95/46 as the most important instrument. Article 8(2) Charter is – in turn – based on secondary data protection law, in particular Directive 95/46. This means that the interpretation of the right to data protection under Article 8(2) Charter draws on the acquis as laid down in Directive 95/46. This reasoning is circular, since the European Court of Justice interprets Directive 95/46 in light of Articles 7 and 8 Charter. Moreover, there is no clear demarcation line between the right to data protection as such (a right guaranteed under primary EU law) and the rights established in secondary EU law.

The relationship between Article 16(1) and 16(2) TFEU is also not clear. Article 16(2) does not only create an obligation to lay down rules on data protection, but also an obligation to lay down rules on the free movement of data. Chapter 6 will elaborate on the presumption that the addition of the free movement of data does not have an autonomous meaning, although this is not evident on the basis of the Treaty’s text. The same goes for the addition

---

916 Conclusions of Chapter 2.
917 Conclusions of Chapter 3.
918 Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 8.
919 E.g., Joined cases C-92/09 and C-93/09, Schecke and Eiffert, EU:C:2009:284; Case C-291/12, Schwarz, EU:C:2013:670, at 25, Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12) EU:C:2014:238. See Chapter 2, Section 13 of this study.
920 According to Syrpis, this is a wider problem and not strictly related to privacy and data protection; Phil Syrpis, “The relationship between primary and secondary law in the EU”, CMLR (2015), 461–487.
“within the scope of EU law” in Article 16(2) TFEU, in relation to processing by the Member States. This addition is presumed to be meaningless.921

Furthermore, Article 16(2) TFEU – and its similarly worded equivalent in Article 8(3) Charter – establishes control by the independent data protection authorities. Under Directive 95/46 – and confirmed by the European Court of Justice – this control is an essential component of data protection.922 This presumes that – under Article 16(1) TFEU – an individual has a right that control of the processing of his data is ensured. It is however not clear to what extent he can invoke this right before a court without having to rely on secondary law.

The exercise of the rights to privacy and data protection and the limitations of these rights require separate attention. Chapter 2 described data protection not as a right to prevent processing of personal data, but as rules of the game for data processing in a system of checks and balances. This qualification of the right to data protection has consequences for the Court of Justice’s assessment of the interference of the right, including the proportionality test. The processing of personal data is not by definition an interference of the right that must be justified. However, Chapter 2 also concluded that this qualification of data protection must not weaken the right, which is a fundamental right under primary EU law and assessment should take place in light of the Charter. This is a matter where legal clarity is needed.

### 3. The Institutional Role of the CJEU in the Constitutional Order of the EU

Article 19(1) TEU establishes the role of the Court of Justice of the European Union, with an implicit reference to the rule of law. The Court must ensure that in the interpretation and the application of EU law the law is observed. It also provides for judicial redress against EU institutions and bodies.923 The Court has jurisdiction in the proceedings specified in the Treaty on the Functioning of the European Union.924 As a result of the decentralised structure of judicial redress, individuals do not – as a rule925 – have direct access to the Court. They have to invoke their rights before a national court, which may – and sometimes must – refer a question of EU law to the European Court of Justice.926 The Court ensures a complete system of judicial review.927

The CJEU acting as a constitutional court with three functions: the review of fundamental rights, market integration and umpire between the different powers

---

921 As explained in Chapter 6, Section 2 of this study.
924 As laid down in Articles 263-273 TFEU.
925 The main exception is laid down in Article 263(4) TFEU.
926 Article 267 TFEU.
The Court of Justice of the European Union is not just an instance for dispute settlement, but it is also characterised as a constitutional court. This constitutional role implies a balancing between the powers of the Union and the Member States, and developing constitutional principles of judicial review.

Stone Sweet identifies three functions for this constitutional role, based on a contribution of Shapiro in 1999: market integration, umpire between various powers and the review of fundamental rights. This study changes the order and discusses mainly the review of fundamental rights. The protection of fundamental rights is the core of this study and respect for privacy and data protection by the European Court of Justice constitutes the main substance of this chapter. A change of order is also justified since Shapiro wrote his contribution before the enactment of the Charter of Fundamental Rights of the European Union.

The first function, discussed in this chapter, is ensuring the review of the fundamental rights. The review of the fundamental right to privacy and data protection by the Court of Justice means in the first place an interpretation of the scope and nature of the right to data protection under Article 16(1) TFEU and of the exceptions and limitations to these rights. The review extends to the balancing with other fundamental rights and public interests. Privacy and data protection are guaranteed at the constitutional level. The Court interprets the rights and the EU legislator is bound by the interpretation of the Court. In a number of cases, the Court interprets Directive 95/46 in the light of Articles 7 and 8 Charter. If the EU legislator does not agree with the ruling of the Court, it can change the directive, but this cannot result in overriding the interpretations of the Court on the scope and nature of the fundamental rights, or on the balancing with other fundamental rights and public interests.

The second function in the role of the Court of Justice is ensuring that the commitment to integration in the Treaties is delivered. Although this function mainly relates to market integration, it is also relevant in other fields. The Member States need a constitutional court to ensure that they stick to their commitment in the Treaties to integrate their markets and do not fall back to protectionism. Member States have discretion in the implementation of EU law, but this discretion should not impede the commitment in the Treaties from being realised. Here the role of the Court is to enforce that Member States comply with their obligations under EU law, mainly in cases where the European Commission starts infringement proceedings against a Member State under Article 258 TFEU or where a national judiciary sends a preliminary reference to the Court under Article 267 TFEU.

\[\text{References:}\]

928 Weiler in: Gráinne de Búrca, J.H.H. Weiler (eds), The European Court of Justice (Oxford University Press, 2001), at 218.
929 Paul Craig and Gráinne de Búrca, EU Law, Text, Cases and Material (fifth edition), Oxford University Press 2011, at 61-66 (including the references made there).
930 AG Jacobs, as quoted in: Paul Craig and Gráinne de Búrca, EU Law, Text, Cases and Material (fifth edition), Oxford University Press 2011, at 65.
932 As explained in Chapter 2, Section 13 of this study.
example of a case where the Court limited the discretion of the Member States in the area of data protection is *ASNEF and FECEMD*. The integrationist approach can be seen as a natural tendency in the review by the Court and is also in the interest of the Member States. The Court aims at assuring the Member States that other Member States adhere to the rules.

As a third function, a constitutional court is needed as an umpire where decision-making powers are fragmented between the European Union and the Member States and at the level of the Union among the EU institutions. The European Court of Justice fulfils this function where it is called upon to adjudicate on the legal basis of an EU instrument, in cases where the competence of the Union to act is challenged. In a wider sense, the Court fulfils the role of umpire between the various governmental actors in the field of data protection, for instance where the jurisdiction of an independent data protection authority in a certain Member State is challenged.

*The perception of an activist CJEU*

These three functions are elements that shape the task of the Court of Justice of the European Union, also in the field of privacy and data protection. In the exercise of its role the Court is often perceived as activist, which was especially the case in the years of stagnation of the Union, when the Court pursued an approach of legal integration, meaning that it enhanced the effectiveness of EU law and promoted the integration of EU law in the national legal order. Its approach is also characterised as teleological or purposive.

An activist role – or more modestly worded: an evolutionary role – of the European Court of Justice is particularly relevant where the legislative process is paralysed. One example Spahiu gives is the deadlock in the recast of Regulation 1049/2001 on public access to EU documents because the European Parliament and the Council did not manage to agree on a

---

933 Joined cases C-468/10 and C-469/10, *ASNEF and FECEMD*, EU:C:2011:777
936 This was, e.g., the case in Case C-230/14, *Weltimmo*, EU:C:2015:639.
938 Paul Craig and Grainne de Búrca, *EU Law, Text, Cases and Material* (fifth edition), Oxford University Press 2011, at 64.
The Court filled the gap in law-making by taking a protective approach limiting the exceptions to public access.\textsuperscript{942}

This – perceived – activist role qualifies the Court of Justice as a suitable actor for privacy and data protection on the internet, since these fundamental rights are challenged on the internet with its inherent cross-border nature, big data and mass surveillance.\textsuperscript{943} Safeguarding privacy and data protection on the internet may require an activist approach, promoting effective protection of these essential values under EU law. This approach may also be relevant under the regime of the General Data Protection Regulation,\textsuperscript{944} for instance if the regulation’s compliance with the level of protection under the Charter were to be challenged.

\textit{Strengths and weaknesses in the role of the CJEU}

The Treaties provide for a full system of legal protection in which preliminary references by national courts play a central role. The preliminary ruling procedure under Article 267 TFEU is the ‘jewel in the Crown’ in the jurisdiction of the Court of Justice of the European Union and of seminal importance for the development of EU law.\textsuperscript{945}

This study demonstrates that this appreciation of the procedure under Article 267 TFEU also extends to the area of privacy and data protection, since most of the rulings discussed in this study stem from preliminary proceedings. The exception is the case law on the independence of data protection authorities,\textsuperscript{946} which is the result of infringement proceedings instigated by the European Commission under Article 258 TFEU. The case law on the relationship between privacy and data protection and public access to documents – with \textit{Commission v Bavarian Lager}\textsuperscript{947} as the leading case\textsuperscript{947} – is, on the whole, the result of direct actions on the review of the legality of EU institutions’ acts under Article 263 TFEU.

The success of the preliminary ruling procedure is particularly apparent given the fact that the recent landmark cases of the European Court of Justice in the area of privacy and data


\textsuperscript{943} As explained in Chapter 3.

\textsuperscript{944} Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.

\textsuperscript{945} Paul Craig and Grainne de Búrca, \textit{EU Law, Text, Cases and Material} (fifth edition), Oxford University Press 2011, at 442.


protection – *Digital Rights Ireland and Seitlinger*, digital rights Ireland and Seitlinger, *Google Spain and Google Inc.*, and *Schrems* – were all three the outcome of this procedure.

The strength of the Court’s contribution is at the same time its main weakness. Any judicial authority cannot set its own agenda, is dependent on the cases brought before it and cannot adjudicate of its own motion. The Court’s contribution to the respect of the right laid down in Article 16(1) TFEU is the consequence of the institutional role of a judiciary in a democratic society. Moreover, the Court cannot enforce compliance by Member States without an infringement act by the European Commission or a preliminary reference by a national court.

In view of this ‘passive’ role, the case law of the Court of Justice is by definition incremental. It is not the Court’s role to develop a policy, let alone a comprehensive policy, for better protection. The Court cannot provide for remedies either: this is a task of the Member States. Moreover, there is limited control on the implementation of the Court’s case law, in particular in preliminary rulings. In infringement procedures, under Article 260(1) TFEU, a Member State should take the necessary measures to comply with the Court’s ruling. If a Member State fails to do so, the European Commission may start a new procedure under Article 260(2) TFEU in which it will propose a pecuniary penalty.

4. The Legitimacy of the CJEU: Compensating for the Presumed Democratic Deficit of the EU

The legitimacy of the Court of Justice of the European Union is beyond doubt, because the Court of Justice is the highest constitutional court of the Union. The Court fulfils the tasks assigned to it by the Treaties. Considering that primary EU law – and more specifically the Treaty on European Union – is the highest authority, the Court must ensure that the commitments made in primary EU law are respected.

---

948 Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger* (C-293/12) and *Seitlinger* (C-594/12), EU:C:2014:238.
951 As explained by Lenaerts, the President of the Court of Justice, at: http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/.
952 To reinforce the CJEU’s role it is therefore important that individuals – and data controllers – are empowered to bring cases before a national court. The proposed General Data Protection Regulation addresses this issue to a certain extent. E.g., any body, organisation or association that aims to protect data subjects’ rights and interests concerning the protection of their personal data will be entitled to a judicial remedy (Article 76(1) of the Commission Proposal).
954 Stone Sweet also mentions the advantage: the CJEU is less likely to produce bad policy; A. Stone Sweet in: Paul Craig and Grainne de Búrca (eds), *The evolution of EU Law* (second edition), Oxford University Press 2011, at 129.
955 Article 19(1) TEU.
Furthermore, the European Court of Justice has legitimacy because of its close link with national courts, in particular through the cooperation in the preliminary ruling procedure. This cooperation was conceived as a horizontal relationship in which the Court of Justice and national courts were separate but equal. Over the years this relationship has become more vertical, with a stronger position for the Court. This allies with an argument by Gerards that the Court does not pay sufficient respect to national constitutional traditions and to national legislative and policy choices.

However, in terms of legitimacy, the fact that national courts are tied to the European Court of Justice in a relationship that – arguably – has vertical elements is less sensitive than subjecting national administrative authorities to the European Union. Within the Union, courts are, by definition, politically neutral and do not aim at realising the polities of democratically elected majorities. A strong position of the Court of Justice does not limit the freedom of the governments of the Member States in the political domain.

Chapter 4 of this study addressed the legitimacy of EU action, in connection with the democratic deficit of the European Union and the aspect of accountability to elected majoritarian bodies. Democratic legitimacy is not an issue for a judiciary that, in a democracy based on the separation of powers, has a task in counterbalancing the preferences of political majorities, and ensuring the respect of essential values in a society. Neither the Court of Justice nor any other court should be held accountable before democratic institutions.

In contrast, an extensive role of the Court of Justice of the European Union does compensate to a certain degree for the presumed democratic deficit of the Union. Although the EU structures may not provide for satisfactory democratic control of the EU institutions, individuals do enjoy judicial protection, ultimately guaranteed by the Court. The Court contributes significantly to the legal certainty of individuals, by delivering justice and safeguarding the rights of individuals. This is an advantage of development of the law by the judiciary. Courts argue on the basis of case law and do not make sudden changes in jurisprudence because of changes in political preferences.

---

957 Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material (fifth edition), Oxford University Press 2011, at 433.
961 Irma Spahiu, “Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union”, (2015) 31(80) Utrecht Journal of International and European Law 5, at 20. She, e.g., refers to Dworkin, expressing the view that it does not matter courts are not elected, as long as they deliver.

173
**Legitimacy: the CJEU’s constitutional role requires some nuancing**

However, this positive view of the legitimacy of the Court of Justice’s constitutional role should be nuanced. To start with, it creates what Stone Sweet calls a potentially explosive problem: “Constitutional Courts cannot perform their assigned tasks without making law”⁹⁶³ leading to the judicialisation of EU law-making and EU governance and bringing the Court into the political battlefield.⁹⁶⁴ As Kelemen says, the fragmentation of power in the European Union between its various institutions has enhanced the power and assertiveness of the Court.⁹⁶⁵

Moreover, what the European Court of Justice decides does not necessarily receive societal support, and does not necessarily reflect societal consensus.⁹⁶⁶ De Búrca even challenges whether the Court’s approach, which she describes as a self-referential, formulaic and minimalist style of reasoning, is appropriate for adjudicating fundamental rights.⁹⁶⁷

These nuances are also reflected in a reaction to *Google Spain and Google Inc.*⁹⁶⁸ De Hert & Papakonstantinou argue that in the former case the Court of Justice stretched the wording of Directive 95/46 so broadly that this justifies the question whether the Court should, instead, not better have referred the matter to the legislator.⁹⁶⁹ A first reaction to *Schrems⁹⁷⁰* by Kuner could be understood as supporting the views of de Búrca. Kuner blames the Court for having a lack of interest in the ruling’s practical effects, also for the global context.⁹⁷¹

Furthermore, Stone Sweet argues that the integrationist approach plays a central role in the reasoning of the European Court of Justice. In its essence, an integrational approach means that when the Court balances the interest of EU integration with national interests it gives preference to the former. Stone Sweet links this approach to the Court’s own interest to maximise coherence of EU law. According to him, this approach is meant to give the Court itself more legitimacy.⁹⁷²

---

⁹⁶⁵ R. Daniel Kelemen, Suing for Europe, Adversarial Legalism and European Governance, Comparative Political Studies, Volume 39 Number 1, February 2006 101-127, at 105.
This argument is relevant in relation to the Court’s task of ensuring the respect of the fundamental rights to privacy and data protection. As this chapter demonstrates, an important contribution of the European Court of Justice is the balancing of privacy and data protection with another right or public interest that, predominantly or in its entirety, falls within a Member States’ competence, such as the freedom of expression or safeguarding security. If the Court were to take an integrationist approach in this balancing exercise, this would favour privacy and data protection. The argument – which is solely presented for a better understanding of the context – is that by strengthening privacy and data protection, the Court would also enhance EU integration.

However, this hypothesis of an integrationist approach is not based on empirical evidence. On the contrary, based on research of case law, Schwarze claims that the European Court of Justice has successfully balanced EU integration and the legitimate interests of Member States.973

This study takes the view that the Court enhances its legitimacy by properly balancing the interest of EU integration and national interests. The requirement of proper balancing – in accordance with the principle of subsidiarity – is relevant in several parts of this study. However, this does not mean that the result of the balancing is always similar. On the internet, the importance of EU integration may weigh stronger than national interests, for instance in the interest of the digital single market.974 Moreover, where privacy and data protection are particularly affected by developments in the information society, a proper balancing may require a different approach to compensate for this impact.975

Effectiveness: the CJEU contributes to bridging the gap between principles and practice

In its case law, the Court of Justice of the European Union does not only require that other actors in the EU legal order – be it Member States or institutions – respect the principle of effectiveness, but it also adjudicates itself in full respect of this principle. In the recent case law we have seen that the principle of effectiveness was a driving force setting high standards for privacy and data protection on the internet.976

A further issue is the extent to which the European Court of Justice can actually contribute to the effective exercising of the right to data protection, in view of the limitations to its role, as discussed above. In this context, a comparison with the right of access to EU documents under Article 15 TFEU can be made. The Court has contributed significantly to the content of

---

973 J. Schwarze in: The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law - La Cour de Justice et la Construction de l’Europe: Analyses et Perspectives de Soixante Ans de Jurisprudence, Various Editors, published by the CJEU on the unique occasion of its 60th anniversary, at 274.
975 This is, arguably, the approach of the CJEU in Case C-131/12, Google Spain and Google Inc., EU:C:2014:317; see Section 13 of this chapter.
976 See, again, Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
the right of access to documents. By doing so, it has bridged the gap between general principles and practice. The same cannot be said – yet – for privacy and data protection, also because of the relatively limited number of cases adjudicated until now. However, the number of cases on data protection is growing significantly, and the Court of Justice plays a key role in the interpretation of the rights to privacy and data protection, as the case law referred to at various places of this study shows.

The more fundamental question is whether bridging this gap is a realistic ambition in the area of privacy and data protection. As has been discussed in Chapter 2, privacy is a rather complicated legal concept: it must be applied in a wide variety of situations, both in the public and in the private sector, and the balancing of the various interests is context-specific. Under such circumstances the Court of Justice provides guidance, where it adjudicates in cases explaining EU data protection legislation in view of Articles 7 and 8 Charter. In order to bridge the gap between general principles and practice, other mechanisms also need to be provided by the legislator and the independent data protection authorities, on the basis of Article 16(2) TFEU.

5. Until the Lisbon Treaty: Emergence of Fundamental Rights in the EU Legal Order

This section describes the fundamental rights protection by the Court of Justice of the European Union as a general framework for the Court’s contribution to the respect of the rights to privacy and data protection. The section highlights the changing role of EU law, in relation to national (constitutional) law and the European Convention on Human Rights. EU law is becoming more prominent in a domain that traditionally was dominated by national law, subject to the ECHR.

Connection to fundamental rights under national law

Constitutions of EU Member States bear witness of the importance of fundamental rights for our democracies, under the rule of law. For example, the preamble of the French Constitution proclaims the adherence to the Rights of Man as defined by the Declaration of human and civic rights of 1789, Article 1 of the German Constitution guarantees human dignity, human rights and the legally binding force of basic rights, and the Dutch Constitution opens with a chapter on fundamental rights.

---

978 In Chapter 2, Sections 8 and 9.
979 The principle of accountability as explained in Chapter 6, Section 14 is an example.
980 “Le peuple français proclame solennellement son attachement aux Droits de l'homme et aux principes de la souveraineté nationale tels qu'ils ont été définis par la Déclaration de 1789, confirmée et complétée par le préambule de la Constitution de 1946 [...].”
981 “Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Das Deutsche Volk bekennt sich darnach zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt [...]”
Although the Treaty of Rome of 1957 did not refer to fundamental rights, these rights have from an early stage of EU integration been recognised as an integral part of the general principles of EU law, protected by the European Court of Justice. Initially, there was a close connection to fundamental rights recognised and protected by the constitutions of Member States, since the Court was “bound to draw inspiration from constitutional traditions common to the Member States”. This initial approach was closely linked to the supremacy of EU law, in order to assure the Member States and their courts that the supremacy would not adversely affect the respect for fundamental rights.

The Court of Justice also underlined that a possible infringement of fundamental rights by an EU measure can only be judged in the light of EU law itself. In Hauer, the Court explains this position by arguing that, if EU measures were permitted to be reviewed in the light of national concepts of fundamental rights, this review could damage the substantive unity and efficacy of EU law, and could lead “inevitably to the destruction of the unity of the Common Market and the jeopardizing of the cohesion of the Community.” In other words, the Court felt obliged to rule itself on possible infringements of fundamental rights, as part of its task of ensuring a uniform interpretation of EU law. There is a parallel with the recent ruling in Melloni. In this case, the Court considered that – in a specific situation – applying a higher standard of fundamental rights protection under national law could undermine the supremacy of EU law.

Besselink argues that the Member States’ courts – and in particular the German constitutional court – triggered the protection of fundamental rights within the EU’s own legal order, because the Court of Justice needed to demonstrate that it ensured the protection of fundamental rights in a satisfactory manner. However, the Court did not fully achieve this result. The Solange I ruling of the German Bundesverfassungsgericht of 1974 is telling in this respect. The German constitutional court did not accept the supremacy of EU law as such, but only accepted supremacy so long as [solange] the EU legal order lacked a written catalogue of fundamental rights. More precisely, the German constitutional court claimed...

982 A catalogue of fundamental rights was originally foreseen in the 1950s, in connection to the ambition of setting up a European Political Union. However, the result was more limited: the European Economic Community (1957). Further read: Grainne de Búrca in Paul Craig and Grainne de Búrca, The evolution of EU Law, Second Edition, Oxford University Press 2011.


986 Case C-399/11, Melloni, EU:C:2013:107, in particular at 55-62.


989 The ruling also mentioned the democratic deficit. The rulings of the German constitutional court on the relation between the two legal orders are described in European Union Law, Koen Lenaerts and Piet van Nuffel, Third edition, 2010, at 779-786.
that – in the absence of such a catalogue – it was entitled to review EU legislation in the light of the protection of fundamental rights.

A systematic review of EU law, in light of the ECHR

The European Court of Justice did not only refer to fundamental rights as principles under Member States’ law, but it equally took international treaties into account, especially the European Convention on Human Rights. In 1974, the Court ruled in Nold II: “Similarly, international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories, can supply guidelines which should be followed within the framework of Community law.”990 In 1991, the Court added in the ERT case that the ECHR has special significance in that respect: “The Community cannot accept measures which are incompatible with observance of the human rights thus recognized and guaranteed.”991 In the following period, the Court systematically reviewed EU law in light of the ECHR, as part of case law in which fundamental rights protection was gradually stepped up.992

Whereas the relevance of the ECHR increased in the case law of the Court of Justice, other sources of international human rights law only played a marginal role.993 This did not change after the entry into force of the Lisbon Treaty.994 Moreover, there is no consensus as to whether the increased relevance of the ECHR also significantly increased the level of protection. Commentators state that this was not the case.995 An indication supporting this view is the fact that the Court remained reluctant in annulling EU instruments for reasons relating to the violation of fundamental rights, apart from the specific subject of antiterrorist lists.996

Before the entry into force of the Lisbon Treaty: an increasing role of fundamental rights, but Article 7 and 8 Charter are only mentioned once

The respect for fundamental rights – as general principles of EU law – was first laid down in primary law in the Treaty of Maastricht of 1992, which included an Article F (now Article 6) in the (at the time new) EU Treaty. This article codified the case law of the European Court

991 Case C-260/89, ERT, EU:C:1991:254, at 41. The CJEU refers to Case C-222/84, Johnston, EU:C:1986:206, para. 18, in which the CJEU already mentioned the principles on which the ECHR was based.
996 Such as in Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461.
of Justice and referred to the rights guaranteed by the European Convention on Human Rights and the constitutional traditions common to the Member States.

In 1999, the European Council concluded that “the fundamental rights applicable at Union level should be consolidated in a Charter and thereby made more evident.”\footnote{Cologne European Council, 3-4 June 1999, Conclusions of the Presidency, pt 44 and Annex IV.} The European Council does not only refer to the rights of the ECHR and the constitutional traditions common to the Member States, but also states that the Charter should include the fundamental rights that pertain only to the Union’s citizens and that account should furthermore be taken of economic and social rights.

The EU catalogue of fundamental rights, mentioned by the German constitutional court in Solange I, finally emerged with the adoption of the Charter of Fundamental Rights of the European Union. The Charter was first solemnly proclaimed in 2000 as a non-binding instrument, after long discussions amongst the EU institutions. These discussions related to two possible paths of reinforcement of fundamental rights protection: accession by the Union to the ECHR,\footnote{Accession is unlikely in the very short term, CJEU, Opinion 2/13 EU:C:2014:2475.} and a catalogue of rights at EU level.\footnote{See on this: G. González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series 16, 2014, at 185-198.}

The catalogue of fundamental rights uses wordings that differ from the wording used in the ECHR. It also introduced new rights which are not included in the ECHR. The case of privacy and data protection is a good example in this respect. Article 7 Charter is more or less similar to Article 8 ECHR, but in a slightly different wording, whereas Article 8 Charter introduced a new right to data protection, closely linked to the right to privacy.\footnote{These two rights are the main subject of Chapter 2 of this study.} Until 1 December 2009, the Charter did not have binding force.

In the drafting process of the Charter special attention was given to the challenges of the information society and technological innovation.\footnote{Communication from the Commission on the legal nature of the charter of fundamental rights of the European Union, COM (2000) 644 final, at 2.} In its Communication on the Charter’s legal nature of 2000, the Commission underlined that this instrument “sets forth rights which, without being strictly new, such as data protection […], are designed to meet the challenges of current and future development of information technologies”.\footnote{See: G. González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series 16, 2014, at 190-194. See also Chapter 2, Section 10.}

The Charter gradually became more important in the case law of the European Court of Justice, in the beginning leading to legal uncertainty,\footnote{G. González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series 16, 2014, at 214. She states it is difficult to argue that the Charter had rendered EU fundamental rights more predictable.} because the Charter was an additional source of fundamental rights law which did not replace other sources. The Court regularly referred to the Charter, underlining that the Charter was solemnly proclaimed by the European Parliament, the Council and the Commission, and that the principal aim of the
Charter, as is apparent from its preamble, is to reaffirm “rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States”. Articles 7 and 8 Charter on privacy and data protection were mentioned by the Court only once, in *Promusicae*.

However, in many other cases before 1 December 2009, where a possible violation of fundamental rights was at stake, the Court of Justice did not refer to the Charter. The first case on the Directive 95/46 on data protection is a good example: in *Österreichischer Rundfunk* – a case concerning the communication and publication of salaries and pensions of staff of a public body exceeding a certain level, together with the names of the recipients – the Court interpreted the directive directly in the light of Article 8 ECHR and the case law of the European Court of Human Rights. The Court simply stated that the activity concerned falls within Article 8 as interpreted by the ECtHR, given that under Article 8 ECHR activities of a professional nature are not excluded from the notion of private life. In this respect, *Österreichischer Rundfunk* reflects a more general tendency to refer to the case law of the ECtHR.

Despite the absence of a reference to the Charter in most cases, the protection of fundamental rights played an increasing role in the case law of the European Court of Justice, following a growing number of cases in which violation of fundamental rights was pleaded as a ground. This development is the consequence of the mentioning of fundamental rights – and particularly the ECHR – in the EU Treaty. The development also results from the fact that the scope of EU law has extended to areas which intrinsically affect fundamental rights, such as the areas of freedom, security and justice and obviously also data protection. Finally, the proclamation of the Charter presumably will have played a role.

### 6. The Charter since the Entry into Force of the Lisbon Treaty: A Fundamental Change of Approach of the CJEU

---

1004 Case C-540/03, *European Parliament v Council of the European Union*, EU:C:2006:429, at 38, on the right to family reunification. In this specific case the CJEU also drew attention to the fact that the specific directive at stake mentioned Article 7 Charter in its recitals. In Joined cases C-402/05P and 415/05P, *Kadi and Al Barakaat*, EU:C:2008:461, at 335, the CJEU mentions that the Charter reaffirms the principle of effective judicial protection.

1005 Case C-275/06, *Promusicae*, EU:C:2008:54, at 64.

1006 Even in landmark cases on fundamental rights, such as C-112/00, *Schmidberger*, EU:C:2003:333. See more in general: G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series 16, 2014, at 226-229.

1007 Joined cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, EU:C:2003:294, at 73.


1010 This is what the CJEU mentions itself: *Article 8 ECHR “is among the fundamental rights which, according to the Court’s settled case-law, restated by the Preamble to the Single European Act and by Article 6(2) EU, are protected in Community law”; Case C-60/00, *Carpenter*, EU:C:2002:434, at 41.
Since the entry into force of the Lisbon Treaty in 2009, the Charter has the same legal value as the Treaties (Article 6 TEU). This changed status of the Charter is fully reflected in the case law of the Court of Justice of the European Union. The Charter has become an essential parameter for the Court’s assessment of cases: the Court confirms that the Charter has become the principal basis for ensuring that fundamental rights are observed. Moreover, the Charter has reinforced the role of fundamental rights in the Court’s reasoning. All in all, the Court has significantly increased the level of protection of fundamental rights since 1 December 2009.

A general outline of the fundamental rights assessment by the CJEU based on Article 52(1) Charter

Article 52(1) Charter provides the general rule for the limitation of the rights included in the Charter, allowing two categories of justifications: objectives of general interest recognised by the European Union, and the need to protect the freedoms and rights of others. These categories are widely formulated, but – as observed earlier – the application of grounds of justification is always subject to a proportionality test. “Rights and freedoms of others” encompasses the other rights in the Charter itself.

As Prechal explains, the test is not necessarily equal in both situations. Where a balance must be struck between a fundamental right and an objective of general interest, the proportionality test described below applies. The balancing between two rights or sets of rights may require reconciling various fundamental rights in the Charter, not only assessing the limitation of one right.

The first step in the assessment is that a limitation of a fundamental right must be provided for by law. This is the consequence of what Barak explains: “In a constitutional democracy, a constitutional right cannot be limited unless such limitation is authorized by law.” The second step is that a limitation on the exercise of the rights and freedoms recognised by the

---

1013 By way of illustration, the editorial of the Dutch Section of the International Commission of Jurists, entitled: Het Hof als privacy-waakhond die durft door te bijten (“The CJEU as privacy-watchdog that dares to bite”, NJCM-bulletin 2014/19).
1016 According to the Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, they are also widely meant.
1018 This difference in test plays a role in this chapter, but is not further elaborated in general terms.
1019 Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 52.
Charter must respect the essence of those rights and freedoms, a concept that is not fully clear. This requirement stems from the older case law of the European Court of Justice that the very substance of the rights should not be undermined. It is not always obvious what the essence of a fundamental right entails, as Digital Rights Ireland and Seitlinger demonstrates in relation to the fundamental rights in Articles 7 and 8 Charter. A particularly serious interference with these fundamental rights did not affect the essence.

The essence of a right does not play a big role in the case law of the Court of Justice, probably because in case of a disregard of the essence of a right, according to Article 52(1) Charter, there would, by definition, be a breach of the Charter. There would be no room any more for balancing the various interests at stake. The essence is sometimes referred to, for instance by Advocate General Cruz Villalón in Coty Germany in relation to the right to an effective remedy, although without an explicit indication of what constitutes the essence. It is in this perspective remarkable that the Court of Justice ruled in Schrems that the essence of the fundamental rights to privacy (Article 7 Charter) and to effective judicial protection (Article 47 Charter) was affected. Possibly, this changes the trend.

The proportionality test is key in the case law of the CJEU

The proportionality test includes, on the one hand, an assessment of the necessity of the measure, in the sense that there must be no alternative measures with less impact on the fundamental rights and, on the other hand, a proportionality test strictu sensu, a balancing between the various interests. According to the Court’s settled case law, “the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.”

The Court of Justice mentions a number of factors, such as “the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference”. Furthermore, the strictness of the review should be seen in light of the principle of effectiveness, a general principle of EU law.
Hence, the exceptions and derogations recognised in EU law are interpreted in a restrictive way. However, the proportionality test does not always have the same outcome, since it depends on a number of factors such as the area concerned and the nature of the fundamental right involved, but also on other factors.\textsuperscript{1029} This chapter contains a number of examples of the application of the proportionality test by the Court of Justice of the European Union.

\textit{The Charter as yardstick}

The Charter has become the yardstick for the European Court of Justice in the protection of fundamental rights. As part of primary EU law, the Charter is the primary instrument of reference for the Court where fundamental rights are concerned.\textsuperscript{1030} Neither the European Convention on Human Rights, nor the constitutional traditions of the Member States have that function any more. This does not mean that the ECHR is without meaning in the EU legal framework. Article 52(3) Charter requires that the protection under the Charter shall be at least the same as the protection under the ECHR.\textsuperscript{1031}

\textit{Digital Rights Ireland and Seitlinger}\textsuperscript{1032} illustrates how the Court of Justice uses the Charter as a framework for review. The review took place in accordance with Article 52(1) Charter, which is similar to the review by the European Court of Human Rights in Strasbourg under the ECHR.\textsuperscript{1033} This means that the Court of Justice, as a first step, declared whether or not there is an interference with the rights laid down in Articles 7 and 8 Charter.\textsuperscript{1034} As a second step, the Court assessed whether the interference is justified, whereby the Court – in this specific case – considered that the essence of the rights under Articles 7 and 8 Charter had not been adversely affected\textsuperscript{1035} and the directive genuinely satisfied an objective of general interest.\textsuperscript{1036} As a third step the Court of Justice carried out a proportionality test.

In its ruling the Court of Justice did not only refer to its own case law, but also – and in an equal manner – to case law on Article 8 ECHR.\textsuperscript{1037} De Búrca notes that this referencing to the

\textsuperscript{1029} As explained, on the basis of Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 47.
\textsuperscript{1032} Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 69. See in Dutch: H. Hijmans, De ongeldigverklaring van de dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof, NTER September 2014, no. 7, pp. 245-252.
\textsuperscript{1034} Paras 32-37 of the ruling.
\textsuperscript{1035} This is the difference with Case C-362/14, Schrems, EU:C:2015:650, where the CJEU considered the essence of Articles 7 and 47 Charter to be affected.
\textsuperscript{1036} Paras 38-44 of the ruling. The CJEU also takes into account that Article 6 Charter lays down the right of any person not only to liberty, but also to security.
\textsuperscript{1037} At 35, 47, 54 and 55 of the ruling.
European Convention on Human Rights does not reflect a general practice. She shows that until end 2012 the Court only referred to the ECHR in 18 out of 122 cases involving the Charter. However, the references to the ECHR are the only references to non-EU sources of law the Court makes regularly.

In the area of privacy and data protection several other examples demonstrate that the Charter is the yardstick. We mention Schecke and Google Spain and Google Inc., cases that play an important role in this study for various reasons. In ASNEF and FECEMD, a case on the interpretation of a specific provision in Directive 95/46, the Court of Justice took account of the Charter in ruling that the discretion of the national legislator in specifying a provision of EU law may be limited. In Schwarz, the Court assessed the taking and storing of fingerprints for the European biometric passport on the basis of the Articles 7 and 8 Charter, leading to the conclusion that the pertinent EU regulation could be considered to be proportionate. Finally, in the two most recent cases on the independence of the data protection authorities (Commission v Austria and Commission v Hungary), which are extensively discussed in Chapter 7 of this study, the Court alluded to the fact that the requirement of independence derives from primary EU law, and in particular from Article 8(3) Charter.

In other areas, the same trend can be observed. Test-Achats was a case in the area of non-discrimination. One of the earliest cases demonstrating the importance the European Court of Justice attached to the Charter was DEB Deutsche Energiehandels- und Beratungsgesellschaft, on the right to an effective judicial remedy under Article 47 Charter. Although the Court referred extensively to the similarity of this provision with Article 6 ECHR, it decided the case on the basis of the Charter, taking into account the

1040 Joined cases C-92/09 and C-93/09, Schecke and Eiffert, EU:C:2009:284.
1042 The specific provision is Article 7(f) of Directive 95/46. Joined cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777, paras 37-49. The case has also importance in the context of balancing rights and interests.
1044 To be complete, Chapter 2 mentions two other data protection cases where the CJEU referred to the Charter: Case C-543/09, Deutsche Telekom, EU:C:2011:279, at 49-54, and Case C-212/13, Ryněš, EU:C:2014:2428, at 28.
1045 Case C-614/10, Commission v Austria, EU:C:2012:631, and Case C-288/12, Commission v Hungary, EU:C:2014:237. In the first case, C-518/07, Commission v Germany, EU:C:2010:125, the Charter did not play this role, possibly because the ruling dates from 9 March 2010, only very shortly after the entry intro force of the Lisbon Treaty, while the opinion of AG Mazak was even delivered before the entry into force.
1046 To be complete, the CJEU referred in the same way to Article 16(2) TFEU.
1047 Case C-236/09, Association Belge des Consommateurs Test-Achats, EU:C:2011:100.
1048 Case C-279/09, DEB Deutsche Energiehandels- und Beratungsgesellschaft, EU:C:2010:811.
principle of effectiveness under EU law.\textsuperscript{1049} In \textit{Otis and others},\textsuperscript{1050} the Court ruled that Article 47 Charter secures in EU law the protection given by Article 6 ECHR. Hence, it sufficed to refer to Article 47.

Another clear example, of a slightly different nature, is \textit{N.S.}\textsuperscript{1051} which relates to the Common EU Asylum System. The Court of Justice decided that an EU instrument that provides for the transfer of an asylum seeker from one Member State to another should be set aside if there are substantial grounds for believing that there are systemic flaws in the asylum procedure and the reception conditions in the receiving Member State,\textsuperscript{1052} breaching Article 4 Charter. In other words, the EU instrument was not affected, but it could not be applied by Member States for reasons of systemic breach of the Charter.

\textit{The Charter has a wide scope, but does not extend the competences of the EU}

The scope of application of the Charter has its limits.\textsuperscript{1053} First, as laid down in Article 51 thereof, the Charter, cannot have the effect of extending the competences and tasks of the European Union, under the principle of conferral.\textsuperscript{1054} In \textit{Torralbo Marcos}, the European Court of Justice clarified: “Where a legal situation does not fall within the scope of Union law, the Court has no jurisdiction to rule on it and any Charter provisions relied upon cannot, of themselves, form the basis for such jurisdiction.”\textsuperscript{1055} Second, the Charter only applies to the Member States when implementing EU law. However, within these limits, the scope of application to the Member States is wide, as was clarified by the Court in \textit{Åkerberg Fransson}\textsuperscript{1056}. As Advocate General Sharpston summarised: “[…] the test is whether the situation is one in which EU law applies (that is, one that falls ‘within the scope of EU law’) rather than (perhaps more narrowly) whether the Member State is ‘implementing’ EU law by taking specific positive action.”\textsuperscript{1057} In \textit{Åkerberg Fransson} the Court also considered that where an action of the Member States is not entirely determined by EU law (so partially falls outside the scope of EU law), national authorities and courts remain free to apply national standards for fundamental rights protection, provided that the level of protection provided by the Charter is respected.\textsuperscript{1058} In short, where EU law applies the Charter applies and the Charter determines the minimum level of protection.

\textsuperscript{1050} Case C-199/11, \textit{Otis and others}, EU:C:2012:684, at 47.
\textsuperscript{1051} Joined cases C-411/10 and C-493/10, \textit{N.S., and M.E. and Others}, EU:C:2011:865. This case is particularly important because it nuances the notion of mutual trust between the Member States. Mutual trust is a rebuttable presumption. See Chapter 4, Section 6.
\textsuperscript{1052} At 86 of the ruling.
\textsuperscript{1053} Further read: ‘Judicial review of Member State action under the general principles and the Charter: Defining the “scope of Union law”’, 52 CMLR, Michael Dougan, Issue 5, pp. 1201–1245.
\textsuperscript{1054} Article 51(1) Charter also mentions the principle of subsidiarity.
\textsuperscript{1056} Case C-617/10, \textit{Åkerberg Fransson}, EU:C:2013:280.
\textsuperscript{1057} Opinion in Case C-390/12, \textit{Pfleger}, EU:C:2013:747, pt 41. In her opinion in Case C-34/09, \textit{Zambrano}, EU:C:2010:560, pt 163, she pleaded for an even wider scope, namely the existence and scope of a material EU competence, even if such a competence has not yet been exercised. This idea was not followed by the CJEU.
\textsuperscript{1058} At 29 of the ruling.
The wide scope of application of the Charter has even further implications for the Member States, as becomes clear from *Melloni*, a case relating to the European arrest warrant. Within the scope of EU law, Member States are not always free to require a higher level of protection. In *Melloni* the European Court of Justice ruled – in a specific situation where an exhaustive EU regime exists – that applying a higher standard would undermine the supremacy of EU law, because applying this higher standard by a Member State would have as an effect that an EU legal instrument that fulfils the requirements of the Charter cannot be applied. The specific situation related to Council Framework Decision 2002/584/JHA on the European arrest warrant, which was modified in order to neutralise the inconsistent way in which the Member States dealt with the consequences of trials where the person concerned does not appear in person. This modification aimed at harmonising these consequences, in full respect of fundamental rights. In such a situation, a Member State cannot require a higher fundamental rights standard, jeopardising the goal of harmonisation.

Under *Melloni*, there may be situations where the Charter – despite its Article 53 – does not only determine the minimum, but also the maximum level of protection. This is for instance the case in certain cross-border situations. *Melloni* has been criticised for this wide understanding of the Charter, which even prevailed over fundamental rights included in the national constitution of Spain.

### 7. The Test under the Charter is Strict and considers a Number of Factors

In *Digital Rights Ireland and Seitlinger* the Court of Justice of the European Union, for the first time, declared an EU instrument entirely invalid, because it interfered with a fundamental right. The review by the Court was strict and, as a consequence, it ruled that the EU legislator had exceeded the limits imposed by the principle of proportionality. Following an observation that the instrument was appropriate for attaining its objective, the Court

---


1061 Article 1(2) of Council Framework Decision 2009/299/JHA (OJ L 81/24), predating the Lisbon Treaty, refers to Article 6 TEU, not to the Charter. However, the CJEU based itself on the Charter.

1062 Article 53 provides: “Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised […] by the Member States’ constitutions.”


1065 This in itself is arguable, since – as, e.g., mentioned in para. 50 of the ruling – the effectiveness is not fully ensured.
explained in a comprehensive reasoning why the EU legislature had exceeded its discretionary power.\textsuperscript{1066}

The European Court of Justice held in this case that, by adopting Directive 2006/24 on data retention\textsuperscript{1067} the EU legislature had exceeded the limits imposed by the proportionality principle in the light of Articles 7, 8 and 52(1) Charter.\textsuperscript{1068} The interference with a fundamental right was so serious that the EU legislature’s margin of discretion was reduced, with the result that review of that discretion would be strict. The Court mentioned a number of factors which played a role in reviewing the validity of the directive. These factors are: “the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference”.\textsuperscript{1069}

This ruling is the more or less logical consequence of an approach, which started with \textit{Schecke} and \textit{Test-Achats},\textsuperscript{1070} in which the Court exercised “stringently its function as the EU’s own constitutional court.”\textsuperscript{1071}

\textit{Schecke, Test-Achats, and Google Spain and Google Inc: three cases of stringent testing by the CJEU}

In \textit{Schecke},\textsuperscript{1072} the Court of Justice ruled that certain provisions – so not the entire legal instrument – of an EU regulation on the publication of information on natural persons receiving aid from EU agricultural funds were invalid. The Court first underlined that increasing the transparency of the use of the funds pursued an objective of general interest recognised by the European Union.\textsuperscript{1073} It then noted that the provisions were appropriate for attaining the objective pursued, since the information made available to citizens reinforced public control of the use to which that money was put and contributed to the best use of public funds.\textsuperscript{1074} Subsequently, this objective must be reconciled with the fundamental rights set forth in Articles 7 and 8 Charter.\textsuperscript{1075}

It is in the latter context that the Court of Justice of the European Union develops a stringent proportionality test. The EU legislator is obliged to balance, before disclosing personal data,
the Union’s interest in guaranteeing the transparency of its actions with the infringement of the rights recognised by Articles 7 and 8 Charter. The legislator should examine alternatives, and no automatic priority can be given to transparency. Both in Schecke and in Digital Rights Ireland and Seitlinger, the nature of the rights to privacy and data protection played an important role in determining the test’s strictness.

The same stringent test was applied in Test-Achats, in which the Court of Justice also decided to declare a provision of an EU law instrument invalid, because of its incompatibility with the Charter, in particular with Article 21 on non-discrimination and with Article 23 on the equality between men and women. The invalid provision allowed Member States to derogate from a prohibition to use sex as a factor in the calculation of certain financial benefits. The Court reached its verdict despite the fact that the derogation was subject to certain conditions. For the Court, it was decisive that the Member States were allowed to maintain the derogation without temporal limitation.

Another example of a stringent test is Google Spain and Google Inc. In this case the Court took account of the seriousness of the interference with the data subject’s fundamental rights under Articles 7 and 8 Charter in deciding that the operator of a search engine has a wide responsibility for the links to webpages it provides.

The same strict test does not necessarily extend to all fundamental rights under the Charter

The nature of the fundamental right is not the only relevant factor for the Court of Justice, but this factor does seem to make a difference. Case law relating to the fundamental rights, included in Articles 15-17 Charter, illustrates this point. These fundamental rights are: the freedom to choose an occupation and the right to engage in work, the freedom to conduct a business and the right to property. Sky Österreich is a case on compulsory access to a satellite signal to enable a public broadcasting company to make short news reports. The Court ruled that the freedom to conduct a business may be subject to a broad range of interventions on the part of public authorities which may limit the exercise of economic activity in the public interest.

In Pfleger, a case on machines for games of chance, the Court of Justice answered preliminary questions on the compatibility of a national law with the freedom to provide services under Article 56 TFEU and with Articles 15-17 Charter. In its ruling, the Court analysed the national law at stake under Article 56 TFEU and added a few considerations on

---

1076 At 83-85 of the ruling.
1077 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 48.
1078 Case C-236/09, Association Belge des Consommateurs Test-Achats, EU:C:2011:100.
1080 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317, at 69-81. See on this case also Sections 12 and 13.
1081 Case C-283/11, Sky Österreich, EU:C:2013:28, at 46.
1082 Case C-390/12, Pfleger, EU:C:2014:28.
the Charter. Its main message is that what is unjustified or disproportionate under Article 56 TFEU is not permitted under the Charter either. In other words, the Charter – in particular Article 16 thereof – has no added value here. One could argue that this reasoning of the Court is the consequence of Article 52(2), which provides that the Charter does not alter the system of rights recognised under the former EC Treaty, but this argument does not explain the relatively lean test applied to Article 16 Charter on the freedom to conduct a business.

Admittedly, the Court of Justice adopted this position in view of the circumstances of the case. In *UPC Telekabel Wien*, on the blocking of access by an internet service provider to copyright-protected films, the Court took a different approach and interpreted Article 16 Charter in a more substantive manner. However, the ruling in *UPC Telekabel Wien* does not contradict *Pfleger*, since the test under Article 16 Charter is not very strict.

8. The Notion of Fundamental Rights: Different Methods of defining Fundamental Rights are useful for understanding Fundamental Rights

The notion of ‘fundamental rights’ comprises notions such as ‘human rights’ and ‘civil and political rights’. The European Court of Justice initially used the term ‘fundamental human rights’. The main convention in Europe is the European Convention on Human Rights, whilst on 19 December 1966, the General Assembly of the United Nations adopted an International Covenant on Civil and Political Rights (ICCPR). All these rights are first generation fundamental rights and have a primarily negative character since they require governments to refrain from acting.

The notion of ‘fundamental rights’ also includes ‘social rights’ such as the rights contained in the European Social Charter and the Community Charter of the Fundamental Social Rights of Workers. These are called ‘second generation fundamental rights’ and require governments to act. In the EU legal order, the fundamental freedoms guaranteed by the Treaties that ensure free movement within the European Union are considered to be

---

1083 See mainly para. 50 of the ruling.
1084 Article 52(2) as explained in the Explanations relating to the Charter of Fundamental Rights (OJ (2007) C 303/17) on Article 52.
1085 C-314/12, *UPC Telekabel Wien*, EU:C:2014:192, at 49: “The freedom to conduct a business includes, inter alia, the right for any business to be able to freely use, within the limits of its liability for its own acts, the economic, technical and financial resources available to it.”
1086 In this context it is illustrative that the CJEU initially used the term ‘fundamental human rights’; e.g., case C-29/69, *Stauder*, EU:C:1969:57, at 7. It is worth noting that in Dutch a similar term is used (“fundamentele rechten van de mens”), but that in most other language versions no equivalent can be found.
1087 The recitals of the Covenant state that for the ideal of free human beings, conditions must be created whereby everyone may enjoy his or her civil and political rights.
1088 See J.H. Gerards, ‘Fundamental rights and other interests – should it really make a difference?’, in: E. Brems (ed.), Conflicts between Fundamental Rights, Antwerp: Intersentia 2008, p. 655-689; C. Fabre, Constitutionalising Social Rights, *The Journal of Political Philosophy*: Volume 6, Number 3, 1998, pp. 263-284; and the references mentioned in both papers. This categorisation of the rights is much more subtle, as will be explained below in Section 9.
1089 As referred to in Article 151 TFEU.
fundamental rights. The notion of ‘fundamental rights’ suggests that it relates to something special that is more than a claim relating to social or economic interests. However, this suggestion does not describe what fundamental rights are.

A positivist method of defining fundamental rights

One could define fundamental rights in a positivist way, which in the EU legal order would mean that the term encompasses all the rights mentioned in the Charter of Fundamental Rights of the European Union. The Charter contains a relatively long catalogue of fundamental rights, in 50 articles. A positivist method qualifying all Charter rights as fundamental rights reflects the primacy and the autonomy of the system of EU fundamental rights’ protection, as recognised by the Court of Justice in Kadi and Al Barakaat. However, this method would also reflect what is often called a proliferation of fundamental rights. Arguably, if more rights need protection, the level of protection will be weakened.

The Charter does not distinguish between fundamental rights. The only distinction the Charter makes is between rights and principles. Article 51(1) Charter provides that rights shall be respected and principles observed. This distinction is supposed to mean that principles cannot be directly invoked before a court, but that they require implementation. Ladenburger mentions two paradigms relating to the principles in the Charter. Either they are objective norms addressed to the state, or they are principles needing implementation. However, these explanations are of limited use. In the first place it is not always clear whether a provision of the Charter contains a right or a principle. In the second place this distinction is not absolute, since many rights also require legislative implementation in order to be effective. The right to data protection is an example. This is why Article 16(2) TFEU requires legislative instruments.

A definition of fundamental rights by their nature of moral value

The reasoning of the CJEU in Case C-112/00, Schmidberger, EU:C:2003:333, may imply that the CJEU places the right to free movement on the same level as a human right. See also Section 9 of the chapter.


Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, at 282-285.


The Explanation on Article 52 only gives limited guidance. Moreover, the distinction between rights and principles was not included in the original Charter text. See on this: M. Borowski in: The Treaty of Lisbon and the Future of European Law and Policy, eds M. Trybus and L. Rubini, 2012, at 210.

A second method to define fundamental rights is based on their nature. As observed earlier, fundamental rights have a special character – or in any event a perceived special character – that distinguishes them from other interests. Fundamental rights reflect values in society, which are of a different nature than claims concerning social or economic interests.

Human dignity is such a value which is capable of distinguishing fundamental rights from other societal interests. This is also how the Fundamental Rights Agency defines fundamental rights: “Fundamental rights set out minimum standards to ensure that a person is treated with dignity.” Habermas calls human dignity “the moral source from which all the basic rights derive their sustenance”. Fundamental rights must protect individuals against attacks on their dignity.

Human dignity as a concept is usually linked to civil and political rights, but it also covers social rights to the extent they are aimed at guaranteeing – minimal – conditions for a decent life. A society should take care of sick, elderly and poor people. A topical example would be ensuring minimum reception conditions for refugees. In general, however, social rights are more linked to ideals of equality than of human dignity.

According to the Explanations relating to the Charter of Fundamental Rights, “none of the rights laid down in this Charter may be used to harm the dignity of another person, and that the dignity of the human person is part of the substance of the rights laid down in this Charter.” Dignity – as well as the integrity of the person – are, at least according to the Explanations, the basic values underpinning all fundamental rights, although in the Charter itself the Title on dignity only relates to a few absolute rights, such as the right to life, prohibition of torture and of slavery and forced labour.

Autonomy is another moral value which forms the basis for the protection of fundamental rights. Fabre explains that autonomy – the control people have over essential elements of
their life – gives protection of fundamental rights special status. This applies to civil and political rights, but also to social rights, since persons need resources to have control over their lives.

Also for society, the fundamental rights reflect essential values. For example, the preamble of the European Convention on Human Rights mentions that fundamental freedoms are the foundation of justice and peace in the world. The preamble also underlines the universal nature of these rights.

The added value of this second method is that it enables courts to focus on more essential rights, in terms of dignity of the persons concerned and the foundations of a democratic society. However, this method, too, has a downside: there is a tendency, in particular in the case law of the European Court of Human Rights,1109 to give these rights a wide interpretation which weakens the focus. In the areas of privacy and data protection, a good example is Niemietz,1110 a case in which the ECtHR extended the right to private life to the right to establish and develop relationships with others, including, to a certain extent, professional and business activities.

The historical method: establishing the fundamental nature of rights using their backgrounds

A third method is to derive the fundamental nature of the right from its historical background. Fundamental rights are political and civil rights of individuals, protecting them against the state. These are the first generation rights included in the European Convention on Human Rights and in the International Covenant on Civil and Political Rights of 1966, which can to a certain extent be seen as a reaction to the atrocities in the Second World War, and are also based on the idea of human dignity.1111 This is reflected in the preamble of the Universal Declaration of Human Rights of 1947:1112 “Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind”.

The rights to privacy and data protection have a different background, as was explained in Chapter 2. The inclusion of the right to privacy in post-war instruments on fundamental rights is part of the reaction of democratic society to totalitarian regimes. Data protection emerged, as a reaction to modern science and technology, to protect individuals against the possible misuse of personal information, not only by states but also by the private sector.1113

---

1110 Niemietz v Germany, ECtHR (1992), A-251-B, at 29. See also Amann, ECtHR (2000), Application No. 27798/95, at 65.
This example shows that taking the historical background as the point of departure is a useful method, also because it demonstrates that protection of fundamental rights is a dynamic process, depending on time and circumstances. As the European Court of Human Rights repeatedly stated in relation to the ECHR: It “is a living instrument which […] must be interpreted in the light of present-day conditions.”1114 Whereas the focus on fundamental rights after the Second World War was instigated by fear of totalitarianism or similar abuses by European States,1115 this fear is now no longer the driving force – at least not the only driving force1116 for the protection of fundamental rights. Globalisation and technology have changed or at least widened the perspective.

9. Distinctions between Fundamental Rights on the Internet: Towards a Simple Taxonomy

Neither the Charter, nor its Explanations make significant distinctions between fundamental rights, apart from the distinction between rights and principles. There is “rarely any hierarchy between rights.”1117 The Explanations mainly explain the background of the Charter’s articles, which, in quite a few cases, can be found in the European Convention on Human Rights. In Axel Springer v Germany,1118 the European Court of Human Rights does not only declare that the rights to privacy and freedom of expression deserve equal respect, as a matter of principle, but also that the margin of appreciation should in principle be the same in both cases.1119

This study does not argue the opposite, that a hierarchy does exist, but takes the view that distinctions between fundamental rights should be made in an internet environment, whilst taking into account that Axel Springer v Germany only extends to the interaction between privacy and freedom of expression.

Chapter 3 concluded1120 that the internet changes the perspective of the European Union and the Member States. First, the governance structure of the internet is an example of the declining role of the state; second, on the internet fundamental rights increasingly coincide, for example privacy and data protection increasingly coincide with the freedom of expression; third, there is a dependency of the Union and the Member States on private parties resulting from the shift of power towards big companies on the internet; fourth,

1114 E.g., Tyrer v UK, 25 April 1978, Application No. 5856/72.
1116 Article 7 TEU points at the situation of a clear risk of a serious breach by a Member State of EU values, but is not relevant here.
1118 Axel Springer v Germany, Application No. 39954/08, at 87.
1120 See Chapter 3, Section 9.
conflicts of jurisdiction are a phenomenon that is inherent to the internet and should be addressed.

Against this background, it should be recalled that the Court of Justice of the European Union makes a certain difference in the standard of review for various fundamental rights, although this depends on a number of factors. Arguably, if all fundamental rights in the Charter need equal protection, the level of privacy and data protection will be weakened in a complex internet environment. The internet challenges the protection as such, but also requires these rights to be balanced with other fundamental rights because, as observed, fundamental rights increasingly coincide. Moreover, a different standard of review is justified by the fact that not all fundamental rights are equally challenged on the internet. The obvious example is that a free internet promotes free speech, but challenges privacy and data protection. Furthermore, the duty to protect fundamental rights on the internet requires resources. A difference in the standards of protection allows an efficient use of resources, with a focus on the rights which are most important in a democratic society.

Finally, in an internet environment fundamental rights have an inherent extraterritorial effect which may collide with legitimate jurisdictional claims of third countries or international organisations. Extraterritorial application may be legitimate to defend essential values of a society, but not in relation to a wide range of rights and principles. Choices may be needed, also for reasons of legitimacy. The legitimacy of external EU action is also determined by – possibly conflicting – legitimate claims of third countries and international organisations.\footnote{1121}{As explained in Chapter 1.}

Towards a simple taxonomy

In Digital Rights Ireland and Seitlinger, the Court of Justice of the European Union qualified the nature of the rights to privacy and data protection as being an important factor necessitating a strict review by the Court that, in this case, ultimately led to the invalidity of Directive 2006/24 on data retention.\footnote{1122}{At 47 and 48 of the ruling.} In the case law on the freedom to choose an occupation and the right to engage in work, the freedom to conduct a business and the right to property,\footnote{1123}{Articles 15-17 Charter, Cases C-283/11, Sky Österreich, EU:C:2013:28, C-314/12, UPC Telekabel Wien, EU:C:2014:192, and C-390/12, Pfleger, EU:C:2014:281.} the Court’s review was not equally strict. This difference in approach indicates that under the Court’s case law distinctions are made between various categories of fundamental rights. The emphasis on human dignity in relation to fundamental rights, for example in the Explanations relating to the Charter of Fundamental Rights,\footnote{1124}{OJ (2007) 303/17.} is a further indication.

We also recall Schmidberger,\footnote{1125}{Case C-112/00, Schmidberger, EU:C:2003:333, at 76-80. Quote taken from para. 80.} a case on the freedoms of expression and assembly, predating the Lisbon Treaty. According to the Court of Justice, the freedoms of expression and assembly do not appear to be absolute but must be viewed in relation to their social
purpose, unlike other fundamental rights enshrined in the European Convention on Human Rights, such as the right to life or the prohibition of torture and inhuman or degrading treatment or punishment. On the basis of this reasoning, the Court treats the freedoms of expression and assembly in the same way as the fundamental freedoms of the EU Treaty which have an economic background, such as in casu the free movement of goods.

Schmidberger is interesting for a number of reasons. In the first place, the ruling identifies different categories of fundamental rights (absolute rights and rights that may be restricted) and, in the second place, it seems to give the same value to civil and political rights (freedoms of expression and assembly) and to social and economic rights (free movement). This position was made more explicit in an opinion of Advocate General Trstenjak in Commission v Germany of April 2010 stating: “In the case of a conflict between a fundamental right and a fundamental freedom, both legal positions must be presumed to have equal status.”\textsuperscript{1126} As said, Schmidberger predates the Lisbon Treaty and the opinion was issued shortly after its entry into force, so the approach may since have changed.

This study proposes a simple taxonomy of fundamental rights in four to six categories, which should be helpful for privacy and data protection in an internet environment for the four reasons mentioned above: the difference in the standard of review, the balancing between rights, efficient use of resources and the extraterritorial application.

A first category of fundamental rights would be the “non-derogable”\textsuperscript{1127} or absolute fundamental rights, within the meaning of Schmidberger, corresponding to the rights included in Title I of the Charter, entitled dignity. They include the right to human dignity, which is inviolable (Article 1 Charter)\textsuperscript{1128} and which is of a general, potentially far-reaching nature.\textsuperscript{1129} However, as Dupré explains, it is a foundational value, but a notoriously difficult legal concept, and it is seen as a prerequisite for all rights.\textsuperscript{1130}

A second category of fundamental rights is composed of rights which are particularly relevant for human dignity, but not qualified as non-derogable. A good example of a case where a huge impact on dignity was recognised, but where the right at issue could not be qualified as non-derogable, is a ruling on homosexual asylum seekers. The Court of Justice acknowledged that the sexual orientation is a characteristic fundamental to a person’s identity, but that his fundamental right is not \textit{per se} breached by a restricting measure, because a derogation is possible.\textsuperscript{1131} The distinguishing factor of this second category would

\textsuperscript{1126} Opinion AG Trstenjak, C-271/08, Commission v Germany, EU:C:2010:183, at 81. He also argued against the hierarchy of rights. The CJEU followed the opinion, albeit without these statements of principle.


\textsuperscript{1128} Articles 2, 4 and 5 (life, protection against torture and slavery) do not seem to have specific relevance in the context of this study. The right to physical and mental integrity has mainly relevance in medical setting.


\textsuperscript{1131} Hence, the mere existence of legislation criminalising homosexual acts is not sufficient to constitute persecution (in a third country and thus to grant asylum under EU law), whereas risk of imprisonment is
be the impact on the human dignity. At first sight, these second category rights are the fundamental rights included in the first generation fundamental rights instruments, i.e. the civil and political rights that are protected under the European Convention on Human Rights and the International Covenant on Civil and Political Rights. Privacy (and data protection) as well as the freedom of expression and information definitely belong to this category.

A third category comprises the social, cultural and economic rights. This category includes the rights laid down in Articles 15-17 Charter (the freedom to choose an occupation and the right to engage in work, the freedom to conduct a business and the right to property). These rights normally – but not necessarily – require (legislative) action from governments. Three nuances must be made. First, social, cultural and economic rights are characterised as peripheral rights and their nature as fundamental rights may be questioned, but they are not necessarily less valuable in society than civil and political rights, as was explained above. Second, the difference between civil and political rights, on the one hand, and social and economic rights, on the other hand, has become less relevant, due to the wide interpretation of civil and political rights. Third, different views are possible as to the qualification of the right to property, which has a historical link to civil and political rights. This will be explained in Section 15.

Three further categories are distinguished for systematic reasons. The distinctions between these three categories have no specific relevance for this study on privacy and data protection on the internet. A fourth category of fundamental rights that could be distinguished are the principles referred to in Articles 51(1) and 52(5) Charter that cannot be directly invoked before a court, but require implementation. A fifth category are the fundamental economic freedoms of the Treaties, relating to the free movement of goods, services etc. Exceptions are only allowed for overriding requirements in the public interest and need to be duly justified. A sixth category is the undefined species of public and general interests, which could be any interest recognised under the Treaties, or in any event the wide categories of interests meant in Article 52(1) Charter.

The taxonomy could enable the CJEU to elaborate its case law, further strengthening the protection of individuals on the internet.

---


1133 Chapter 2 proposes to consider both fundamental rights as part of one system.


1138 Under the vast case law, in accordance with the standard case C-120/78, Rewe-Zentral (“Cassis de Dijon”), EU:C:1979:42.
Before the entry into force of the Lisbon Treaty, it seemed that the European Court of Justice valued the various rights more or less on an equal footing. The example of Schmidberger showed a balancing between first generation fundamental rights (freedom of expression and assembly) and a fundamental freedom under the Treaties (free movement of goods) without expressing any difference in the importance of these rights. The Court did not address this issue, whereas the referring Austrian Court had asked whether the object of a public demonstration could be considered of a higher order than the free movement of goods. Another example is Promusicae.\textsuperscript{1139} In a case where the effective protection of copyright had to be ensured and had to be balanced with the right to data protection, the Court ruled that a fair balance should be struck between the various fundamental rights at stake without establishing an order between these rights. Advocate General Kokott had proposed a different approach, namely assessing the case as an exception to the right to private life under Article 8 ECHR. She also qualified the protection of copyright as a fundamental interest of society, though not as a fundamental right.\textsuperscript{1140}

After the entry into force of the Lisbon Treaty, the case law of the Court indicates\textsuperscript{1141} that the nature of the right deserving protection does make a difference. However, this case law is not fully clear, also because the nature of the right is not the only factor determining the strictness of review. The taxonomy could enable the Court to develop its case law, further strengthening the protection of individuals on the internet.

10. The CJEU takes a Strict Approach on Privacy and Data Protection, particularly when balancing with other Fundamental Rights, and with the Objective of Security

Section 6 explained that the Court of Justice’s assessment of limitations to a fundamental right focuses on proportionality. The Charter has become the yardstick and has a wide scope, but with limits. The test under the Charter is strict, depending on a number of factors. The nature of the fundamental right is such a factor, as Section 7 specified. Section 8 proposed a taxonomy that could enable the Court to elaborate its case law. These are the starting points of the next sections, on balancing privacy and data protection on the one hand with certain fundamental rights and the public interest of security on the other hand.

The strict approach of the CJEU

The Court of Justice of the European Union takes a strict approach to privacy and data protection, considering the changed reality in the information society and its impact on

\textsuperscript{1139} Case C-275/06, Promusicae, EU:C:2008:54.

\textsuperscript{1140} See in particular points 52 and 105 of her opinion.

\textsuperscript{1141} This does not necessarily mean that the CJEU is consistently applying a new approach. E.g., in case C-314/12, UPC Telekabel Wien, EU:C:2014:192, at 47, the CJEU points at the necessity of striking a balance between the right to conduct a business (Article 16 Charter), the right to property (Article 17 Charter) and the freedom of information (Article 11 Charter) without any differentiation. However, the balancing test by the CJEU remained superficial. The case did not require a more in-depth analysis.
privacy and data protection. Google Spain and Google Inc.\textsuperscript{1142} addressed the loss of control over personal data, in relation to the activities of a search engine and Digital Rights Ireland and Seitlinger\textsuperscript{1143} addressed the consequences of mass surveillance.

These cases demonstrate that the Court of Justice is not only strict, but also specific in explaining privacy and data protection. Where the Court balances privacy and data protection with other fundamental rights and public interests, it has a precise framework for scrutinising data protection, laid down in EU legislation. The Court interprets Directive 95/46 in the light of the fundamental rights of privacy and data protection.\textsuperscript{1144} However, it does not have a similar framework in respect of other fundamental rights and public interests, where the competences are exercised by the Member States.

Chapter 2 of this study explained that privacy is a concept that is interpreted broadly, much wider than the original notion of the right to be left alone, and that it has been extended to the relations with the outside world.\textsuperscript{1145} Privacy is recognised as being a prerequisite for the exercise of other fundamental rights such as the freedom of speech.\textsuperscript{1146} The connection of data protection with other fundamental rights follows from its definition in Council of Europe Convention 108\textsuperscript{1147} and the various EU instruments of data protection\textsuperscript{1148} that refer to other fundamental rights and freedoms.

Privacy and data protection are not absolute rights. Limitations and restrictions are needed, because the European Union and its Member States also need to protect other fundamental rights and public interests. Furthermore, the balancing with other rights and interests is the core of the protection given by the Court of Justice. As explained in Chapter 2, Article 8 Charter provides that personal data must be processed fairly. The Court specifies that data protection itself requires a balancing act.\textsuperscript{1149} The potential harm a limitation of the fundamental right would have for the values a right aims to protect is relevant. Harm is a difficult concept, particularly in relation to privacy and data protection,\textsuperscript{1150} but could be a useful tool in an internet environment where protection is becoming ever more complicated.

Where the Court of Justice balances privacy and data protection with other fundamental rights and public interests it seems to consider that some compensation for the loss of control

\textsuperscript{1142} Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
\textsuperscript{1143} Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
\textsuperscript{1144} As explained in Chapter 2, Section 13.
\textsuperscript{1145} Niemietz v Germany, ECHR (1992), Application No. 13710/88.
\textsuperscript{1146} As Rodota states: “It allows individual beliefs and opinions to be freely made public.” In: Reinventing data protection?, S. Gutwirth, et al. (eds), Springer 2009, p.79.
\textsuperscript{1147} Article 1 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108: “The purpose of this convention is to secure […] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (‘data protection’).”
\textsuperscript{1148} E.g., recital (2) of Directive 95/46.
\textsuperscript{1149} Case C-518/07, Commission v Germany, EU:C:2010:125, at 24.
over personal data in an internet environment may be needed. Hence, this case law of the Court gives a significant boost to internet privacy and data protection. The case law reflects that these fundamental rights aim at preserving dignity and autonomy as conditions for a functioning democratic society, under the rule of law, and that the respect of these rights is at risk in an information society.

*Privacy and data protection have a huge impact on human dignity and effective protection is essential in a democratic society which is subject to the rule of law*

Privacy and data protection qualify as fundamental rights of the second fundamental rights category within the short taxonomy: these rights have a huge impact on human dignity and effective protection is essential in a democratic society. More concretely, this has as a consequence that: (1) there is a necessity of protection in an online environment; (2) where needed, extraterritorial application of the rights must be safeguarded; (3) the rights should be applicable in horizontal relations; (4) restrictions and limitations of these rights are subject to a strict test; (5) where a balance is needed with other fundamental rights and public interests, the essential nature of the rights to privacy and data protection should be taken into account; and (6) this may lead to an approach where the Court adjudicates itself, and does not defer the matter to the national courts (in preliminary ruling procedures).

These six consequences are more than mere explanations of the state of the art in the Court’s case law, especially in view of the challenges posed by the internet. We argue that these consequences should be guiding for the interpretation of the Union’s task under Article 16(1) TFEU to ensure that everyone’s right to data protection is respected. These consequences should also play a role where the EU legislator exercises its task under Article 16(2) TFEU. Moreover, they should be translated into the practices of the independent data protection authorities. The importance of the rights to privacy and data protection may require that they are an element of external EU action.

*Introduction of the following sections*

The following sections will explore the balancing, as provided by Article 52(1) Charter, of privacy and data protection with the most relevant other fundamental rights and the public interest of security, in the context of an information society. This focus on the connection

---

1151 See mainly Chapter 2 of this study.
1152 As developed in Chapter 6 of this study.
1153 Chapter 7 of this study.
1154 Chapter 9 of this study.
1155 As explained in Section 6, there is a difference between balancing two fundamental rights in the Charter and balancing a fundamental right with a general interest that, under Article 52(1) Charter, is considered as a limitation of a fundamental right.
1156 This chapter does not discuss all other potentially affected fundamental rights mentioned in the Explanatory Memorandum of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final, at 3.3, for reasons that it focuses on fundamental rights that may conflict with data protection. Article 16 Charter on the right to conduct a business is discussed together with the right to property, and Article 21 Charter on non-discrimination is discussed in Chapter 6, because of its parallel with data protection. Article 24 on the rights of the child and Article 35 on health care are not addressed.
with other fundamental rights and with security is at the heart of the entire study. The balancing with other rights and interests is part of the governance of data protection and determines the boundaries of the Union’s competences under Article 16 TFEU.

First, we put the case law of the Court of Justice into a wider perspective, by discussing certain examples of the balancing of interests by the US Supreme Court. The subsequent sections elaborate the distinctions between fundamental rights based on the value that a fundamental right aims to protect, by giving higher status to the rights that aim at preserving human dignity as a condition for a functioning democratic society. The sections consider the impact the developments in the information society have on the exercise of fundamental rights. The exercise of the rights to privacy and data protection has become more complicated in an internet environment, which has an effect on the balancing. The Court seems to acknowledge this in Google Spain and Google Inc.\footnote{1157 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317, particularly in paras 58 and 80. See: Hielke Hijmans, Right to have links removed: Evidence of effective data protection, Maastricht Journal of European and Comparative Law, 2014(3).}

Although there is no explicit hierarchy among fundamental rights under EU law, we submit that distinctions can nevertheless be made and that this is relevant in balancing between various rights and interests, for three reasons: the standard of review, the balancing between rights and the extraterritorial application. These distinctions enhance the legitimacy of data protection, whereas the compensation in the Court’s case law for the loss of control over personal data in an internet environment enhances the effectiveness.

\section*{11. Case Law of the US Supreme Court: Balancing with Free Speech and Security}

This section succinctly highlights two aspects of the case law of the US Supreme Court with particular importance for privacy and data protection on the internet, namely the balancing between free speech and privacy, and the protection of privacy in relation to security. The aim of this section is to put the case law of the Court of Justice of the European Union into perspective and to show that there are differences in substance that are relevant to the external context, as will be further described in Chapter 9, but that there are also similarities.

The ruling of the EU Court of Justice in Google Spain and Google Inc.\footnote{1158 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317, further discussed in Sections 12 and 13.} was heavily criticised in the US,\footnote{1159 See, e.g., Editorial New York Times, 14 May 2014, http://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?_r=0.} because of its presumed adverse impact on the freedom of speech. This criticism can be understood in light of the wide protection given to free speech under the First Amendment of the US Constitution, even where individuals’ privacy may be affected. In Sorrell v. IMS Health Inc.,\footnote{1160 No. 10-779 131 S.Ct. 2653 (2011).} the US Supreme Court held that a Vermont statute restricting the sale, disclosure, and use of records that revealed the prescribing practices of individual doctors violated the First Amendment rights of pharmaceutical manufacturers and
data miners to whom the records were sold. These records contain personal information of the prescribing doctor as well as details of the prescription, including the age and gender of the prescription’s addressee. The name of the patient is not included, but could easily be re-identified. This ruling clearly shows a difference in balancing the various values compared to the EU, giving preference to free speech over the protection of the individual’s privacy, even in a case where the interest of the parties invoking free speech is evidently of a commercial nature.

In United States v Jones (2012) and in Riley v California (2014) the US Supreme Court contributed significantly to the legal development of privacy and data protection in the law enforcement area. There is a parallel to the ruling of the EU Court of Justice in Digital Rights Ireland and Seitlinger, because both courts recognise the changed context of privacy and data protection in an information society. United States v Jones was based on a situation where the police attached a Global Positioning System (GPS) device to the undercarriage of a car; Riley v California dealt with the seizure of a smartphone for law enforcement purposes.

These rulings must be understood in the context of the US Supreme Court’s case law on unreasonable searches and seizures, protected by the Fourth Amendment of the US Constitution. An essential requirement for establishing that there has been a violation of privacy under the Fourth Amendment is that a search or seizure trespasses a protected area, such as a person’s home. The US Supreme Court ruled that this requirement reflects a close connection between privacy and property.

In the already mentioned case of Katz v United States, this requirement was nuanced, since the US Supreme Court rejected the argument that a ‘search’ can occur only when there has been a ‘physical intrusion’ into a ‘constitutionally protected area’, noting that the Fourth Amendment “protects people, not places”. In that case, protection was given in circumstances where government agents had intercepted the contents of a telephone conversation by attaching an electronic listening device to the outside of a public telephone booth. This activity violated the reasonable expectation of privacy of the person concerned.

---

1161 At least that is argued in the Brief of Amici Curiae of the Electronic Privacy Information Center (EPIC) and legal scholars and technical experts, available on: [http://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf](http://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf).
1162 See also Lee A. Bygrave, Data Privacy Law, An International Perspective, Oxford University Press 2014.
1163 132 S.Ct. 945 (2012).
1165 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
1166 To be precise, the Supreme Court used the term cell phone, but emphasised the numerous functionalities of a smartphone.
1167 See also Chapter 2, Section 13.
1168 It is wider, see text of Fourth Amendment.
1169 E.g., United States v Jones, 132 S. Ct. 945 (2012).
1171 Wording taken from the US Supreme Court’s case of Smith v Maryland, 442 US 735 (1979).
Under US law, a person normally does not have a reasonable expectation of privacy in the case of information voluntarily disclosed to third parties. This can go quite far. In *Smith v Maryland*, the US Supreme Court doubted “that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” This reasoning was used as a justification for surveillance conducted by the NSA, since the NSA only kept track of communications data (‘metadata’), not of the content of communications.\(^\text{1172}\) This justification does not concur with EU law, following the ruling of the EU Court of Justice in *Digital Rights Ireland and Seitlinger*, which underlined that the storage of metadata\(^\text{1173}\) could lead to a serious breach of privacy and data protection.

This leads us to the two recent cases of the US Supreme Court mentioned above. In *United States v Jones*, it is foremost the concurring opinion of Justice Sotomayor\(^\text{1174}\) that takes account of the changed context of privacy in an information society. In the first place, she addressed the result of GPS monitoring that makes available at low cost a substantial quantity of intimate information about persons and thus may alter the relationship between individual and government. In the second place, she emphasised that one of the main premises for protection – namely that where information is voluntarily disclosed there is no reasonable expectation of privacy – is not suited to the information society, since persons are constantly revealing information to third parties.\(^\text{1175}\) This concurring opinion reflects a recognition of the fact that on the internet persons constantly leave traces behind, whereas they may expect this information to be treated confidentially.

*Riley v California* is even more important from the perspective of privacy protection in an information society. Mr. Riley was arrested and, upon his arrest, an officer accessed information on his smartphone; in a later stage even more information was found, which was then used in the criminal case against Mr. Riley. The US Supreme Court decided that generally a warrant is needed before a smartphone may be searched, fully realising that the decision would have an impact on the ability of law enforcement to combat crime.\(^\text{1176}\)

The reasoning of the US Supreme Court is most interesting. It acknowledged that smartphones differ in both a quantitative and a qualitative sense from other objects people carry on them, because of their immense storage capacity.\(^\text{1177}\) The Court distinguished the combination of different types of information on the smartphone, the various types of

---


\(^{1173}\) Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* (C-293/12) and *Seitlinger* (C-594/12), EU:C:2014:238; see further Section 17.


\(^{1175}\) Another element of her concurring opinion is a further nuance of the theory of trespassing.

\(^{1176}\) See at 25 of the ruling.

\(^{1177}\) See, in particular, at 17-21 of the ruling.
information by themselves and the history that can be tracked. This wide range of information obviously has consequences for privacy since it reveals much about an individual’s private life. Moreover, the Court mentioned the pervasiveness of smartphones – individuals not carrying one are the exception – and it explained the qualitative changes. Some information did not exist in the past, such as internet search and browsing history, historic location information and apps revealing individuals’ preferences. Finally, the Court mentioned in this perspective links to the cloud.

12. Article 11 Charter on Freedom of Expression and Information: An Intensified Link with Privacy and Data Protection

The freedom of expression and information, which includes the freedom to hold an opinion, is laid down under Article 11 Charter,\(^\text{1178}\) which corresponds to Article 10 ECHR and to Article 19 ICCPR. The freedom does not only include the right to express oneself, but also the right to receive information, as has been confirmed repeatedly by the European Court of Human Rights.\(^\text{1179}\) It is this element of Article 11 that is at the heart of one of the controversies on *Google Spain and Google Inc.*\(^\text{1180}\) The obligation for a search engine to remove a link is said to impinge on the right to receive information.

As the Human Rights Committee of the United Nations states, the freedom of expression and information constitutes a foundation stone for every free and democratic society.\(^\text{1181}\) This freedom is essential, both for individual development and for the society as a whole.\(^\text{1182}\)

Freedom of expression is a first generation fundamental right, which in essence protects the individual against governments. However, the right also contains positive obligations for governments. Governments must ensure effective protection in horizontal situations in order to prevent the freedom of expression from being hampered by acts of private persons and entities.\(^\text{1183}\) Another positive obligation can be read in Article 11(2) Charter that requires the freedom and pluralism of the media to be respected.\(^\text{1184}\)

Both the rights to privacy and data protection and the freedom of expression and information are essential values in our democratic society, and are mutually interdependent. As the European Court of Human Rights ruled in *Axel Springer v Germany*\(^\text{1185}\) the rights are of equal


\(^{1179}\) Article 10 ECHR “guarantees the right to impart information and the right of the public to receive it”, e.g., *Observer and Guardian v the United Kingdom*, 26 November 1991, § 59(b), Series A no. 216).


\(^{1181}\) Human Rights Committee, General Comment No 34 on Article 19 ICCPR, Geneva 2011.


\(^{1185}\) Application No. 39954/08, at 87.
value. Also, the cases Von Hannover v Germany,\textsuperscript{1186} relating to privacy and defamation, illustrate the essential value of these rights and freedoms in a democratic society.

\textit{An intensifying link: three reasons and four concepts}

The link between the rights to privacy and data protection, on the one hand, and the freedom of expression and information, on the other hand, is changing and intensifying in an internet environment. First, the dividing line between private and public speech is becoming blurred, for example as a result of information sharing on social media. Second, changes are caused by the inherent impact of a free and open internet on privacy and data protection, given the fact that a free and open internet facilitates the processing of personal data. This impact is illustrated by the following concepts: the concept of net neutrality entails that end-users must be free to access and distribute information and content, run applications and use services of their choice via their internet access service; the concept of open data encourages sharing of information on open sources, including types of information that were historically protected; the concept of Web 2.0 allows individuals to publish information to the widest public without intermediates. Web 2.0 also entails an abstention of government intervention. Third, new intermediaries – like search engines or providers of social media platforms – play a role in promoting the freedom of expression and information, whereas their responsibilities under data protection law are not yet fully established.

Although these developments relating to the information society\textsuperscript{1187} are positive as such, they nevertheless also increase the risk of facilitating certain undesired effects of the freedom of expression, such as hate speech, harm to minors, or defamation or breaching the privacy of individuals.

\textit{Balancing privacy and freedom of expression, in light of Google Spain and Google Inc.}

Google Spain and Google Inc.\textsuperscript{1188} is a topical example demonstrating that balancing the freedom of expression and information with the rights to privacy and data protection is not evident in an information society. The right to be forgotten – although technically speaking not at stake in Google Spain and Google Inc. and as a term probably an overstatement\textsuperscript{1189} – is the perfect metaphor for demonstrating the complexity of this balancing.

The Court of Justice’s ruling in Google Spain and Google Inc.\textsuperscript{1190} dealt with the interaction and possible collision of privacy and data protection with freedom of expression and information, although the freedom of expression and information was not explicitly

\textsuperscript{1186} Von Hannover v Germany, 2004, Application No. 59320/00 and Von Hannover v Germany (no. 2), 2012, Applications Nos. 40660/08 and 60641/08. See Chapter 2, Section 9 of this study.

\textsuperscript{1187} This has all been explained in Chapter 3 of this study.

\textsuperscript{1188} Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.

\textsuperscript{1189} The ‘right to be forgotten’ never leads to total oblivion. In Google Spain and Google Inc., it is only a right to have certain personal data deleted. See on this also: The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015, https://drive.google.com/file/d/0B1UgZshetMd4eEi3SjJvV0hNbDA/view.

\textsuperscript{1190} Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
mentioned by the Court. Instead, the Court balanced the interests of privacy and data protection with the legitimate interests of the search engine and those of internet users in having access to information. Much of the controversy surrounding the case concerns precisely the relationship between privacy and freedom of expression. The ruling was, for instance, heavily criticised in the US, because of its presumed adverse impact on the freedom of speech. To a certain extent, this controversy was even instigated by the fact that the Court did not mention the freedom of expression, although the interest of the internet user to have access to information through a search engine is quite similar to the right to receive information under Article 11 Charter.

The Court of Justice gave effect to a right that has acquired a reputation as ‘the right to be forgotten’ and that has led to strongly polarised views. Strictly speaking, this right does not exist under current law. The Court adjudicated on the basis of the right to erasure of data under Article 12 of Directive 95/46. Although technically speaking the Court’s ruling has a much more limited dimension, namely the deletion of a link on a search engine (the contested information remains available on the internet, only the access to this information becomes more complicated), it has provoked a further public discussion on the right to be forgotten. Those who take the perspective of privacy and data protection consider it to be an essential innovation to deliver protection in an information society, whereas others consider it as an incentive for censorship on the internet.

Where an individual under Articles 7 and 8 Charter is entitled to request the deletion of information, this automatically has an impact on the right to receive information under Article 11 Charter. The request for deletion also has an impact on individuals exercising their freedom of expression, equally under Article 11 Charter. Anyone uploading information onto the internet – comprising personal data – becomes a controller responsible for compliance with data protection rules, including the deletion of data when asked.

This case enables a better understanding of the balancing between fundamental rights. The ruling was the result of a complaint by a Spanish resident – Mr. Costeja González – against

---

1191 Paras 81 and 97 of the ruling.
1192 See Section 11 above.
1194 The right is included in Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final, as a right to be forgotten and to erasure (Article 17).
1195 Only the referring Spanish Tribunal mentions the right to be forgotten in its preliminary questions.
1196 Paul Bernal even wrote a ballad of Google Spain for the International Journal of European Law, endorsed by Joseph Weiler. See: http://www.ejiltalk.org/the-ballad-of-google-spain/
1198 Taken from: Hielke Hijmans, Right to have links removed: Evidence of effective data protection, Maastricht Journal of European and Comparative Law, 2014(3).
the fact that when his name was entered in Google Search, relatively old pages of a Spanish newspaper were displayed. On these pages, his name was mentioned in relation to the recovery of social security debts. As Mr. Costeja González claimed, the issue had already been resolved a number of years before\textsuperscript{1199} and the data were now entirely irrelevant. They should thus be made inaccessible. The Court of Justice ruled that under these circumstances Mr. Costeja González had a right to obtain that the information relating to him be no longer linked to his name in the list of results following searches on the basis of his name.

Mr. Costeja González invoked his rights against a search engine, not against the publisher of the website displaying the now irrelevant information.\textsuperscript{1200} This allowed the Court of Justice to underline that the activity of the search engine affects the rights to privacy and data protection more significantly than the original source of information, which is logical, since no one would normally consult the publication in the Spanish newspaper anymore. In addition, the processing by the publisher of the website may fall within the derogation in Directive 95/46 for journalistic purposes.\textsuperscript{1201}

13. \textit{Google Spain and Google Inc. restores a Balance, but raises Questions of Legitimacy}

First, the European Court of Justice took into consideration\textsuperscript{1202} the new reality in the information society that has an impact on privacy and data protection, in particular what the Podesta Report calls the persistence of data. Data, once created, is effectively permanent.\textsuperscript{1203} Moreover, it is ubiquitously available, so it can be accessed through other sources than the publisher’s website. Therefore, the only effective way to receive protection is the removal of the link on a search engine.

Second, the reality of internet may have an impact on the protection that is given and on the balancing between fundamental rights. The ubiquitous availability of information affects (or harms) the data subject – at least in the circumstances of the case –, but does not adversely impact the right to receive information. On the contrary, the internet facilitates the access people have to information.\textsuperscript{1204} In these circumstances – as a rule – the right of the data subject prevails as a result of the Court’s ruling, but this does not change the balance between privacy and data protection and the freedom of expression.\textsuperscript{1205} What the Court did was to restore a perturbed balance. The Court considered that the general public had a justified

\textsuperscript{1199} The CJEU’s ruling comes 16 years after the initial publication.
\textsuperscript{1200} At 84-85 of the ruling.
\textsuperscript{1201} Article 9 of Directive 95/46 on data protection.
\textsuperscript{1202} The ruling also raises questions as to the territorial scope of EU data protection law. This is discussed in Chapter 9 of this study.
\textsuperscript{1203} Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (Podesta Report), May 2014, at 9.
\textsuperscript{1204} See also Chapter 3, Section 9.
\textsuperscript{1205} This argument is not shared by all commentators. See e.g.: Stefan Kulk and Frederik J. Zuiderveen Borgesius, Google Spain v. González: Did the Court Forget About Freedom of Expression? September 4, 2014, European Journal of Risk Regulation (2014).
interest in access to information that may overrule the rights to privacy and data protection, for example when the data subject is a public figure.

Third, the ubiquitous availability of information implies a lack of control of data subjects, and therefore affects their autonomy. It has become normal practice for a search engine to disseminate information on any individual, solely based on a reference to the name of that individual in a search request, without having the consent of the individual involved or informing him or her. It is difficult to reconcile this practice with a raison d’être of the right to data protection, which is to give an individual control over his personal data. This confirms one conclusion of Chapter 2 of this study, namely that data protection is not a right to prevent processing of personal data; it is a claim based on fairness.

Fourth, the Court referred implicitly to the right to receive information, but did not address the freedom of expression and information itself, as guaranteed by Article 11 Charter. Authors argue that the ruling affects the freedom of expression by publishers, because delinking by search engines makes their publications harder to find, and also because search engines themselves benefit from the freedom of expression. In any event, the Court considered the importance of search engines in a developing information society, as a condition for the exercise of freedom of expression, but linked this to the responsibility to ensure privacy and data protection.

The fifth issue relates to the differentiation based on the value a fundamental right aims to protect. It is remarkable that the Court placed the economic interest of the search engine and the interest of the general public to receive information, which is, as said, closely linked to the freedom of expression and information (Article 11 Charter) on the same level. This reasoning of the Court does not correspond with the specific role of fundamental rights in a democratic society. A possible explanation is that the Court did not consider the freedom of expression and information because it was not included in the questions by the referring tribunal.

Finally, as a result of Google Spain and Google Inc., search engines now have the responsibility for balancing between different fundamental rights: privacy and data protection on the one hand and the freedom of expression – although, as said, not explicitly mentioned by the Court – on the other hand. This responsibility requires difficult policy judgements on questions like: After how many years can one claim that information should be removed? Which role in the public life of the data subject qualifies as relevant in order to legitimise the continuous linking to information by a search engine?

1206 Frederik Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting, Kluwer Law International 2014, at 3.3. See also Chapters 2 and 3 of this study.
1207 See the conclusions of Chapter 2.
1208 Apart from a reference to Article 9 of Directive 95/46, the derogation for journalistic purposes under Article 9 of Directive 95/46.
1210 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
1211 Further read: Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015
The CJEU no longer takes a deferential approach

In Satamedia\textsuperscript{1212} – a ruling delivered before the entry into force of the Lisbon Treaty – the European Court of Justice had to deal with the derogation for journalistic purposes under Article 9 of Directive 95/46. The Court chose for a deferential method: whilst emphasising the need for balancing required under EU law, the Court left the balancing itself to the national jurisdiction, without providing further guidance.\textsuperscript{1213}

In Google Spain and Google Inc.,\textsuperscript{1214} the Court departed from this deferential method. It explained the obligations of a search engine in light of the Charter, and in particular the obligation to remove – at the request of the person concerned – a certain type of link from the list of results of a search based on the name of that person. The Court gave guidance on how a request for removal should be balanced against the right of the general public to know. As a rule, so the Court stated, privacy and data protection override the interest of the general public to know.\textsuperscript{1215}

Democratic legitimacy is not necessarily guaranteed

This study understands legitimacy, in relation to the governance of data protection, as ensuring that there is some degree of accountability towards political institutions.\textsuperscript{1216} As a result of Google Spain and Google Inc., the search engines now have the task of balancing between fundamental rights, a task which is closely related to one of the core tasks of government in protecting fundamental rights and hence requires high standards of legitimacy to be respected.\textsuperscript{1217} This gives search engines a social responsibility, in a domain where the need for balancing between various interests already challenges the effectiveness of data protection.\textsuperscript{1218} The Article 29 Working Party provides guidance,\textsuperscript{1219} but it is doubtful whether this guidance is sufficient to ensure legitimacy, in the sense of this study.

This hesitation relates to a more general point of democratic legitimacy, where public tasks are exercised by or with the help of private parties. Governments may include non-governmental stakeholders in the governance of privacy and data protection, but this does not

\textsuperscript{1212} Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (Satamedia), EU:C:2008:727.

\textsuperscript{1213} To be complete, the ruling by the Finnish Court ended up with the ECtHR. ECtHR, 23 June 2015, Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland, Application No. 931/13.

\textsuperscript{1214} Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.

\textsuperscript{1215} At 97 of the ruling.

\textsuperscript{1216} As explained by Federico Ferretti, Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?’, CMLR, (2014) 51, Issue 3, pp. 843–868.

\textsuperscript{1217} Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union ruling on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” - WP 225.
mean that the primary responsibility for the protection is also shared with these stakeholders.\textsuperscript{1220}

14. \textbf{Article 42 Charter on the Right of Access to Documents: A Strict Scrutiny but not when balancing with Privacy and Data Protection}

The right of access to documents under Article 42 Charter gives effect to the value of transparency and facilitates democratic control.\textsuperscript{1221} The case law of the Court of Justice of the European Union defined the widest possible public access to documents as being a basic principle.\textsuperscript{1222}

There is a close link between access to documents on the one hand and privacy and data protection on the other hand. Article 4(1)(b) of Regulation 1049/2001\textsuperscript{1223} regarding public access to European Parliament, Council and Commission documents and the case law on the basis of this article\textsuperscript{1224} demonstrate this. In this case law, which balances two (sets of) fundamental rights at the EU level, the Court of Justice underlined that Regulation 1049/2001 and Regulation 45/2001\textsuperscript{1225} on data protection do not contain provisions granting one right primacy over the other. The full application of both regulations should, in principle, be ensured.\textsuperscript{1226}

\textit{Access to documents as a promoter of transparency and good governance}

Transparency means openness in the functioning of governments, in order to promote good governance and ensure the participation of civil society.\textsuperscript{1227} Transparency finds its expression \textit{inter alia} in the right of access to documents, as laid down in Article 15(3) TFEU and Article

\textsuperscript{1220} As explained in Chapter 4 of this study.
\textsuperscript{1222} E.g., Joined cases C-514/07P, C-528/07P and C-532/07P, \textit{Sweden v API and Commission} \textit{(and connected cases)}, EU:C:2010:541, at 73.
\textsuperscript{1225} Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
\textsuperscript{1227} Wording of Article 15(1) TFEU.
42 Charter. Transparency, or openness, extends – subject to limitations - to all parts of governments. This includes authorities which by nature have to respect some degree of confidentiality, in particular services responsible for national security. Openness of these services is not evident, as the Snowden revelations demonstrate. This is why, for instance, Reidenberg proposes that where governments use personal data in the hands of the private sector, this must be logged and made transparent to citizens.

Article 42 Charter on the right of access to documents is closely related to the freedom of expression and information. Both rights and freedoms are essential for a democratic society; they both concern the right of the general public to be informed and they give rise to the same issues in relation to the rights to privacy and data protection. One could interpret access to documents as a species of the right to receive information, which is an element of Article 11 Charter. This interpretation finds support in the case law of the European Court of Human Rights, where a right of access to documents was recognised as part of the right to receive information. In Dennekamp II, the General Court of the European Union referred to Articles 11 and 42 Charter in one go, in ruling on the application of Article 4(1)(b) of Regulation 1049/2001.

However, there are also significant differences between the two fundamental rights and Dennekamp II does not reflect a more general approach of the Court. To start with, access to documents is conceptually linked to good governance, included in Article 41 Charter, which also presupposes that a government should actively give effect to the right. Giving effect to the right of public access to documents requires a government to act – and not to abstain – by handing over information to the citizen, be it spontaneously or on request, taking into account exceptions and limitations to the right as laid down by law.

The scope of Article 42 Charter is limited to documents of the European Union. Article 42 Charter does not extend the scope of Article 15(3) TFEU or Regulation 1049/2001 and does not interfere with the competence of the Member States to ensure public access to the documents their administrations hold. Article 42 Charter, therefore, does not apply to

---

1234 Article 2(4) of Regulation 1049/2001 provides that documents should be made public following a written application or “directly in electronic form or directly through a register. In particular, documents drawn up or received in the course of a legislative procedure shall be made directly accessible.”
Member States when they act within the scope of EU law, as an exception to the general rule laid down in Article 51(1) Charter. Only in specific circumstances – when documents are exchanged between the EU level and the Member States – are the Member States bound by the obligations of the EU regime for public access to documents.

Regulation 1049/2001 is the central piece of EU legislation for access to documents. Article 4 of this regulation provides for the exceptions to public access and has been the object of abundant jurisprudence by the Court of Justice of the European Union. The Court states that the regulation is based on “the principle of the widest possible public access to documents” of the institutions, and that exceptions must be interpreted and applied strictly.1236 Where an exception is made, the EU administration must, in principle, explain how disclosure of a document could specifically and effectively undermine the interest protected by the exception.1237 This requires a case-by-case assessment.1238

However, the same strict approach is not followed when a balance must be struck between access to documents on the one hand, and the rights to privacy and data protection on the other hand, for instance on the basis of Article 4(1)(b) of Regulation 1049/2001.

**Balancing privacy and transparency, in the light of Bavarian Lager**

*Commission v Bavarian Lager*,1239 a case relating to the transparency of documents with lists of participants to professional meetings, can be seen as the example that the balancing does not take place on an equal footing. In *Commission v. Bavarian Lager* the Court of Justice scrutinised the facts of the cases solely on the basis of Regulation 45/2001 on data protection, even on an aspect where there seemed to be a contradiction with Regulation 1049/2001 on public access. Under the latter regulation a right to access can be exercised irrespective of the interest of an applicant in having the document.1240 However, where a document contains personal data, an applicant must “demonstrate the necessity for those personal data to be transferred”.1241 In *Dennekamp v European Parliament*,1242 this requirement prohibited the transfer of information at the request of a journalist, who did not establish why this information was necessary to satisfy the public interest the journalist invoked.

*Dennekamp v European Parliament* sets a high threshold. It is not only necessary that applicants invoking transparency have a specific interest – which can be paraphrased as being the general right of the public to know under transparency rules –, but they must also

---

1236 E.g. Joined cases C-514/07P, C-528/07P and C-532/07P, *Sweden v API and Commission (and connected cases)*, EU:C:2010:541, at 73.
demonstrate necessity. Arguably, this goes beyond the line of the Court taken in Google Spain and Google Inc., where the interest of the general public in finding information may outweigh the right of the data subject, particularly if the latter has played a role in public life, without any reference to necessity in a specific case.

The Court of Justice does not seem to balance privacy and data protection on an equal footing with public access to documents, or wider: transparency. In Schecke, a case outside the scope of Regulation 1049/2001 but dealing with transparency of the EU institutions, the Court followed a similar approach in balancing between these rights and seemed to allow wider exceptions to transparency, when privacy and data protection are affected. The Court ruled that the EU legislator, before allowing disclosure of information relating to a natural person, is obliged to balance the Union’s interest in guaranteeing the transparency of its actions with the infringement of the rights recognised by Articles 7 and 8 Charter. By doing so, the Court assessed restrictions to the rights to privacy and data protection in the Charter motivated by the principle of transparency, as laid down in Articles 1 and 10 TEU and Article 15 TFEU, as well as in Article 42 Charter, without balancing the two rights (or principles) on an equal footing.

This conclusion may be an overstatement, because, arguably, the Court’s case law is mainly the result of the ambiguous wording of Article 4(1)(b) of Regulation 1049/2001. With this nuance in mind, this study takes the view that this case law of the Court confirms that fundamental rights representing human dignity are not balanced on an equal footing with other fundamental rights in the Charter, and that distinctions between fundamental rights can be made.

15. Article 17 Charter on the Right to Property and Intellectual Property: Do these Rights represent Essential Values in a Democratic Society?

According to the Explanations relating to the Charter of Fundamental Rights, the right to property as protected under Article 17 Charter is a fundamental right common to all the constitutions of the Member States. The Court of Justice of the European Union has recognised the right to property in numerous cases. However, the nature of the right to property as a fundamental right was never undisputed. One thing is clear, it is not an absolute right, but it is a right that must be viewed in relation to its social function. The right to property is subject to wide limitations, which follows from Article 17(1) itself. The Union as

1243 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
1244 Joined cases C-92/09 and C-93/09, Schecke and Eiffert, EU:C:2009:284.
1247 Explanations to the Charter of Fundamental Rights, explanation on Article 17, also mentioning the first case, C-44/79, Hauer, EU:C:1979:290.
1248 This is a constant in the CJEU’s case law, before and after the entry into force of the Lisbon Treaty. E.g., Case C-416/10, Križan and Others, EU:C:2013:8.
well as the Member States have a broad margin of discretion in limiting the right to property.\textsuperscript{1249}

Article 17(1) Charter distinguishes between the deprivation of possessions, on the one hand, and regulations on the use of property, on the other hand.\textsuperscript{1250} Deprivation of possessions concerns expropriations in the public interest and, at first sight, does not seem to be relevant for this study. This is different for the regulation of use, which Article 17(1) Charter allows insofar as this is necessary in the general interest.

The Court of Justice leaves the Member States a wide margin of appreciation in regulating the use of property, but limitations of use have to meet the test of proportionality. This margin of appreciation is important in the context of this study, because it may mean that the standard of review the Court applies to the right to property is less strict than the standard it applies to privacy and data protection. In relation to intellectual property, the Court seems to confirm a difference with privacy and data protection. The Court ruled in \textit{Scarlet Extended}\textsuperscript{1251} that there is nothing “to suggest that that right [to intellectual property] is inviolable and must for that reason be absolutely protected”.

This leads to a few remarks on the right to property itself. It is beyond doubt that the right to property has a fundamental nature and relevance in society. The right has a longstanding history. Locke, for instance, emphasised in Two Treatises of Government, the essence of property.\textsuperscript{1252} In his view, every individual has a property in his own person; this is something that nobody else has any right to. This property is linked to his labour. The right to property was also recognised in the American and French revolutions,\textsuperscript{1253} and in those days even linked to civil and political rights. Only – male – citizens having property were considered to be stakeholders in society and were supposed to have a right to vote.\textsuperscript{1254} The limitations on the right to property in parts of Europe before the fall of communism are a further illustration that the enjoyment of the right to property should not be taken for granted.\textsuperscript{1255}

The inclusion of the right to property in the main 20\textsuperscript{th} century international fundamental rights instruments however was less obvious. The right to property is included in Article 17 of the Universal Declaration of Human Rights, but not in the International Covenant on Civil Rights.\textsuperscript{1256} Further read: Ferdinand Wollenschläger on Article 17, The EU Charter of Fundamental Rights, A Commentary, Edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, Hart Publishing 2014, pp. 483-484 and the case law mentioned there.


\textsuperscript{1251} Case C-70/10, Scarlet Extended v Sabam, EU:C:2011:771, at 43.


\textsuperscript{1255} See: https://en.wikipedia.org/wiki/Human_rights_in_the_Soviet_Union#Economic_rights.
and Political Rights. The right to property is not embodied in the European Convention on Human Rights itself, but was only added in the First Protocol to the Convention after much debate. In literature, the right to property is not systematically qualified as a civil or political fundamental right or as a fundamental element of a democracy.\textsuperscript{1256} Gerards calls the right to property a “borderline right”.\textsuperscript{1257} Nevertheless, it is one of the most violated rights of the Convention,\textsuperscript{1258} because of government interference in the peaceful enjoyment by individuals of their possessions.\textsuperscript{1259}

Moreover, the right to property has links with other rights. The European Court of Justice combines this right with the freedom to choose an occupation and the right to engage in work (Article 15 Charter) and the freedom to conduct a business (Article 16 Charter), without specifying their interrelationship.\textsuperscript{1260} In \textit{Pfleger},\textsuperscript{1261} these three provisions are taken together. In \textit{Sky Österreich},\textsuperscript{1262} the obligation of a holder of exclusive broadcasting rights to grant third parties the right to make short news reports is not reviewed under Article 17 Charter as a limitation to the right to property, but as a limitation to the freedom to conduct a business under Article 16 Charter. The Court exercised this review whereas, at the same time, it seemed to indicate that, because of its wording, Article 16 Charter offers less protection than Article 17 Charter. As the Court stated, the wording of Article 16 differs from the wording of other fundamental freedoms and is similar to certain provisions of Title IV of the Charter on solidarity.\textsuperscript{1263}

In short, the right to property is an essential value in a democratic society and recognised as such. However, its status as a fundamental right is ambiguous. The close connection of the right to property with the rights under Article 15 and 16 Charter justifies the qualification of the right to property as an economic right, which aims to protect economic values. However, this qualification does not take into account that the right to property also encompasses a moral value in society, as Locke already underlined.\textsuperscript{1264}

\textit{Intellectual property becomes complicated in the information society and copyright is the example of a right difficult to enforce}

\textsuperscript{1258} See: \url{http://echr-online.com/right-to-property-article-1-of-protocol-1-echr/introduction}.
\textsuperscript{1259} Wording of Article 1 of the Additional Protocol to the ECHR.
\textsuperscript{1261} Case C-390/12, \textit{Pfleger}, EU:C:2014:28.
\textsuperscript{1263} At 46 of the ruling.
\textsuperscript{1264} The moral value of property is also explained by C. Fabre, Constitutionalising Social Rights, The Journal of Political Philosophy: Volume 6, Number 3, 1998, pp. 263-284.
Torremans explains that intellectual property rights were not always considered to be fundamental rights. He describes two schools, one that is based on the presumption of a conflict between fundamental rights and intellectual property rights and a second one that focuses on the interaction and balance between both types of rights. The European Court of Justice followed the second school of thought in Promusicae, by mentioning the need to reconcile the various rights and interests and by giving guidance for the balancing of those rights and interests. This case, which was adjudicated before the entry into force of the Lisbon Treaty, qualified intellectual property as a fundamental right and balanced it on an equal footing with data protection.

Intellectual property rights are based on legislative intervention: laws determine the existence and enjoyment of intellectual property rights. The European Union has adopted an extensive body of legislation on intellectual property rights, mostly based on Article 352 TFEU, which is a supplementary competence that allows the Council to legislate, by unanimity and with the consent of the European Parliament, in a domain where no specific legal basis is provided and if EU action proves to be necessary to achieve an objective of the Treaties.

The information society has an impact on the right to intellectual property. First, the information society complicates the protection and enforcement of intellectual property rights with copyright as the prime example: the information society enables the infinite copying of information and information is ubiquitously available. Moreover, the notion of open data deliberately aims at diminishing the importance of intellectual property.

Second, the relationship between enforcement of intellectual property rights and privacy and data protection was recognised by the EU legislator in Directive 2004/48, but only in a very generic way. On the internet, this relationship gets a new dimension because rights holders develop new methods of enforcement. The mechanisms that are or must be put in place to discourage the illegal downloading of copyright protected materials illustrate the importance of the relationship. These mechanisms could encompass the monitoring of internet users and the filtering and blocking of communications.

In Scarlet Extended, the Court of Justice dealt with a filtering mechanism that required installing a system for filtering that was applied to all customers, as a preventive measure in order to monitor behaviour on the internet for the purpose of protecting copyright. This filtering system “would involve a systematic analysis of all content and the collection and

---

1266 Case C-275/06, Promusicae, EU:C:2008:54, at 65-68.
1268 See Chapter 6, Section 7.
1270 Case C-70/10, Scarlet Extended, EU:C:2011:771. Other cases on this relationship are: Case C-461/10, Bonnier Audio, EU:C:2012:219, and Case C-275/06, Promusicae, EU:C:2008:54.
identification of users’ IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified. In this case, the Court ruled that IP addresses are personal data and considered that the mechanism at stake was not in conformity with EU law, as construed in the light of fundamental rights. The Court observed that a fair balance must be struck between the right to intellectual property and the right to data protection, without specifying the nature of such balancing.

Furthermore, Directive 2000/31 on eCommerce as interpreted by the Court in L’Oréal and others precludes an active monitoring of all customers data in order to prevent any future infringement of intellectual property rights via a provider’s website, albeit for economic reasons not related to fundamental rights. The Court also mentioned that Article 3 of Directive 2004/48 on the enforcement of intellectual property rights has the same consequence.

Does the right to property represent human dignity in the same way as privacy and data protection?

The case law does not give clear guidance as to whether the right to property must be balanced on an equal footing with privacy and data protection. In Scarlet Extended, the European Court of Justice did not deal with this question in any detail, although it did emphasise the non-absolute character of the right to intellectual property.

There are, however, indications in the case law and literature that both (sets of) rights have a different value. Moreover, intellectual property – a subset of the right to property – does not seem to represent the same value. Hence, a tentative conclusion could be that the Court’s case law allows a certain distinction in the level of protection given by fundamental rights, whereby the level is higher for privacy and data protection (and on an equal footing, the freedom of expression and information) in comparison with the protection accorded to the right to property.

---

1271 Case C-70/10, Scarlet Extended, EU:C:2011:771, at 51.
1272 In its ruling, the CJEU also pointed at a number of EU law instruments, also outside the area of privacy and data protection. See also the opinion of AG Cruz Villalón.
1273 Case C-70/10, Scarlet Extended, EU:C:2011:771, at 53.
1274 Important questions remain unanswered; see: Stefan Kulk, Frederik Zuiderveen Borgesius, Filtering for Copyright Enforcement in Europe after the Sabam cases, European Intellectual Property Review 2012, issue 11, pp. 54-58.
1276 Case C-324/09, L’Oréal and Others, EU:C:2011:474, at 139.
1278 Case C-70/10, Scarlet Extended, EU:C:2011:771.
1279 As explained in Section 7.
This tentative conclusion is relevant because the developments in the information society influence the exercise of the right to property, including the right to intellectual property. Examples are the filtering mechanisms put in place to enforce copyright, requiring a monitoring of customers. These developments in the information society illustrate that balancing property and intellectual property on an equal footing with privacy and data protection may weaken the level of data protection when internet monitoring by copyright holders is accepted as a means to protect copyright.


The security of individuals, physical and otherwise, is not recognised in the Charter, but it is an objective of the European Union. For instance, Article 67(3) TFEU provides that the Union shall endeavour to ensure a high level of security. Providing security is a core task of any government. It is the justification of the very existence of the state: it is there to protect life and liberty, or as Thomas Jefferson already wrote in 1776, governments are instituted to secure life, liberty and the pursuit of happiness. The exercise of the rights of privacy and data protection is limited by the task of governments to guarantee their citizens’ security, an objective of general interest in the sense of Article 52(1) Charter.

Privacy and security: a trade-off

The relationship between privacy and security has elements of a trade-off. On the one hand, privacy is seen as inhibiting the appropriate protection of our societies against threats caused by terrorist attacks or by serious crime and, on the other hand, privacy is considered a value that should prevail against the risks of unconditioned surveillance. A trade-off should therefore be made; but how?

One could, for instance, think of a trade-off based on objective data, for instance by balancing surveillance’s negative effects on the essential values of our society with the number of potential casualties if persons were not under surveillance. This is not pure theory. Habermas describes a case – not relating to privacy, but to human dignity – before the German constitutional court, where the German Aviation Security Act, which was adopted following the attacks of 9/11, was declared unconstitutional. The German law authorised German authorities to shoot down passenger aircrafts in situations similar to 9/11. As Habermas explains, the German constitutional court decided in favour of the dignity of the passengers (their right to life) against security of the wider population. This example also shows that this trade-off cannot always be made on a rational basis.

---

1280 In the US Declaration of Independence of 1776.
1281 The trade-off model was the subject of the PRISMS project (not to be confused with PRISM, the programme of the NSA), sponsored by the EU under the 7th Framework Programme; see: http://prismsproject.eu/.
1283 Bundesverfassungsgericht, 1 BvR 357/05 - Ruling of 15 February 2006.
The balancing between privacy and security may in the end boil down to making a comparison between adverse effects on privacy, which can reasonably not be quantified, and imprecise prognoses about casualties in case considerations of privacy and data protection prevail and authorities are limited in the use of personal information. After a terrorist attack – the Paris attacks of January 2015 being a logical example – privacy advocates argue that the attack would not have been prevented if authorities had had more facilities to access data. Persons and authorities responsible for security claim they need more data. Neither side bases its arguments on verifiable figures. The example of terrorist attacks demonstrates the difficulty of a trade-off. It also illustrates that, in these circumstances, arguments based on perceived threats to security tend to be more convincing in the political debate than arguments based on the value of privacy. The argument of privacy is not strong, against an allegation – whether or not based on fact – that it would put the lives of individuals at risk.

The case law of the ECtHR helps understanding privacy, in its relation to security

The European Court of Human Rights has repeatedly ruled on justifications for public authorities’ interferences with the right to privacy under Article 8 ECHR. Various rulings deal with the storing, monitoring and interception of information for police purposes. As illustrated by Digital Rights Ireland and Seitlinger, the European Court of Justice regularly refers to these cases and builds on these rulings when developing its own case law under EU law.

More specifically, the European Court of Human Rights scrutinises the interference of privacy for the purpose of national security. The Court is particularly strict, because a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it. The Court takes account of the lack of public scrutiny in those circumstances and requires adequate and effective measures against abuse. The Court, for instance, insists on clear and detailed rules for the interception of telephone conversations, “specially as the technology available for use is continually becoming more sophisticated.”

The European Human Rights Court also ruled on the interference with privacy in relation to the taking and retention of biometric material of individuals, such as fingerprints and DNA. In S. & Marper, the Court took into consideration the “rapid pace of developments in the field of genetics and information technology”, including “the possibility that in the future

---

1284 MEP Sophie in ’t Veld, reacting on a proposal to facilitate access to PNR data; see: http://www.volkskrant.nl/dossier-europese-unie/tusk-bepleit-haast-met-database-van-vliegtuigpassagiers-naar-eu-a3826625.
1285 E.g., Joint statement issued following a meeting of the ministers of the interior in Paris, 11 January 2015, following Charlie Hebdo.
1286 Klass and Others v Germany, 6 September 1978, paras 49-50, Series A No. 28.
1287 Uzun v Germany, 2010, Application No. 35623/05, a case on the surveillance of GPS data, at 63.
1288 Weber and Saravia v Germany (dec.), Application No. 54934/00, ECtHR 2006-XI, at 93. See also: Liberty and Others v UK, Application No. 58243/00, 2008, at 59-70. In the latter case, the ECtHR ruled that Article 8 ECHR had been violated.
private-life interests bound up with genetic information could be adversely affected in novel ways or in a manner not anticipated with precision today”. 1290

S. & Marper also addressed the issue of discriminatory processing of personal data. The case related to a database with fingerprints and DNA samples taken from individuals in connection with the investigation of an offence, which does not imply that those individuals are (or had been) suspected or convicted. For instance, witnesses were also included. The Court referred to “the risk of stigmatisation, stemming from the fact that persons […], who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons”. 1291 In other words, 1292 a database that is based on discriminatory processing is subject to a strict scrutiny, if the processing could lead to stigmatisation.

Another angle for the assessment by the European Human Rights Court is the relation between a measure interfering with a fundamental right and a concrete security threat. In Nada, the Court took account of the fact that the threat of terrorism was particularly serious at the time of the adoption of certain measures, the period around 9/11. However, that does not give a justification for keeping these measures over the years. 1293

17. The Contribution of the CJEU, with a Focus on Digital Rights Ireland and Seitlinger

In Digital Rights Ireland and Seitlinger, 1294 the European Court of Justice took the case law of the European Human Rights Court relating to privacy and security as the basis for its own scrutiny under Articles 7 and 8 Charter. However, the Court of Justice was even stricter than was required under the case law of the Human Rights Court. In this case, concerning indiscriminate processing of personal data, the Court of Justice expressis verbis reduces the EU legislature’s discretion. 1295 Arguably, this reduced discretion also applies to the national legislature, acting within the scope of EU law. 1296

The Court of Justice struck down Directive 2006/24 on data retention, 1297 a directive requiring Member States to oblige providers of electronic communications (such as telecommunications companies) to retain the traffic data and location data of all electronic

1291 At 122 of the ruling.
1292 At 12 of the ruling.
1293 At 48 of the ruling.
1295 In the wide sense of Case C-617/10, Åkerberg Fransson, EU:C:2013:280; see Section 6 of this chapter.
communications (among which phone calls and text or email messages) of all natural persons in the European Union, for the purpose of the fight against serious crime. The directive excluded the retention of data revealing the content of communications. However, the Court underlined that despite this exclusion, the directive entails an interference with the fundamental rights of practically the entire European population. The instrument was “likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.”

*Indiscriminate retention of data may be appropriate, but remains disproportionate*

The Court based its finding on a range of arguments, some of which allow to draw more general conclusions on balancing privacy and security. The Court even implied that the instrument of indiscriminate retention of communications data as such is not in line with the Charter. The core of the reasoning of the Court relates to the fact that the obligation to retain data applies in an indiscriminate fashion to all individuals, electronic communications and traffic data without differentiation, limitation or exception. It is this indiscriminate nature that makes the obligation disproportional, in the Court’s view.

However, this indiscriminate nature is a key feature of the instrument of data retention. The EU legislature deliberately adopted an instrument to guarantee the availability of historical traffic data of all people in the European Union. This availability of all traffic data allowed law enforcement authorities – after a serious crime was committed – to analyse the communications that had taken place before the crime was committed, to find out more about possible suspects and their networks. This instrument was meant to be effective also in relation to persons who were not yet known to law enforcement authorities. Any less general alternative would not “guarantee the ability to establish [prior] evidence trails […], does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime”.

Whereas the European Court of Justice agreed that this instrument is appropriate for attaining its objective, the instrument nevertheless was considered disproportionate because it requires the retention of data of all Europeans. This could mean that – although the Court did not state this explicitly – any comparable instrument of data retention would fail the proportionality test. Not everyone agrees with this result. Vandamme, for instance, argues that such a far-reaching result is difficult to reconcile with the Court’s view that the essence of the rights to

---

1298 At 56 of the ruling.
1299 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 37.
1300 Required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54, the directive annulled by the CJEU.
1302 See in the same sense: Franziska Boehm, Mark D. Cole, Data Retention after the Judgment of the Court of Justice of the European Union, 30 June 2014, at 92.
privacy and data protection was not adversely affected. More generally, the ruling is interpreted both in a stricter and in a more permissive way.

In addition, the Court of Justice pointed at the lack of clarity in various provisions of Directive 2006/24 on data retention. For instance, the directive did not contain objective criteria to assess whether data access by national authorities is justified, nor did it contain objective criteria to determine how long data should be retained. Other relevant elements were the insufficient level of security prescribed by the directive and the fact that the directive did not ensure the irreversible destruction of the data at the end of the data retention period. Finally, the Court observed that the control by an independent data protection authority, as required under Article 8(3) Charter, was not fully ensured.

This ruling sets the example for a strict scrutiny, within the EU context, of surveillance practices facilitated by the processing of large amounts of personal data for security purposes, which is sometimes characterised as “blanket surveillance”. The ruling confirms the argument defended in this study that the Court is raising the standards of fundamental rights protection.

Despite the vast criticism of Directive 2006/24 on data retention prior to the ruling, judicial authorities, data protection authorities and legal scholars did in general not argue in favour of the invalidity either of the directive or, even more so, of the instrument of indiscriminate retention of telecommunications data as such. For example, the German Bundesverfassungsgericht annulled German national legislation implementing the directive, but did not touch the directive as such, nor did it attack indiscriminate retention.

---

1305 See also Chapter 7, Section 12 of this study.
1307 E.g., European Data Protection Supervisor, Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), OJ C 279/01. The opinion criticises the directive, but accepts the instrument as such.
1309 With an interesting reasoning: because of the broad discretion the directive gave to the national legislator and because it did not govern government access, the directive could be implemented in Germany without infringing the German Basic Law; Bundesverfassungsgericht Germany, Ruling of 2 March 2010, – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, on data retention, Press release No. 11/2010 of 2 March 2010, p. 3. This discretion and the absence of rules on access were decisive for the annulment by the CJEU.
1310 A similar approach was taken by constitutional courts in Bulgaria, Cyprus and the Czech Republic. To the contrary, the Romanian Constitutional Court seemed to be more strict and addressed the retention obligation as such. Further read: Franziska Boehm, Mark D. Cole, Data Retention after the Judgement of the Court of Justice of the European Union, 30 June 2014. See also: Paul M. Schwartz. "Systematic Government Access to Private-Sector Data in Germany“ International Data Privacy Law 2 (2012): 289.
A new dimension to the relation between security and privacy after Digital Rights Ireland and Seitlinger? Four considerations

In Digital Rights Ireland and Seitlinger the European Court of Justice is particularly strict on legal instruments requiring indiscriminate processing, which only allow – or only give the feeling of – indiscriminate surveillance. Schrems\textsuperscript{1311} confirmed this strict approach, given the Court’s consideration that access of public authorities on a generalised basis to the content of electronic communications affects the essence of the right to privacy. This strict approach is not necessarily limited to instruments requiring indiscriminate processing, but may – following the reasoning in S. & Marper, emphasising the risk of ‘stigmatisation’ – also extend to discriminate instruments, which enable targeted surveillance.\textsuperscript{1312}

Digital Rights Ireland and Seitlinger may have consequences in various contexts. Existing instruments involving the processing of large amounts of personal data\textsuperscript{1313} have become vulnerable, whereas, at the same time, proposed instruments that are currently going through the legislative process may come under stricter scrutiny before their adoption by the EU legislature. Proposals with specific relevance in this context are the proposed entry and exit system for third country nationals\textsuperscript{1314} and the proposed directive on an EU passenger name record system.\textsuperscript{1315} External EU action in these areas may also be affected.

The strict approach does not mean that privacy concerns will always override security concerns. The case law of the Court of Justice gives guidance for balancing both concerns, but must be seen in the perspective of the four following considerations.

First, the trends in the two areas: on the one hand, an information society with ubiquitous connectivity and, on the other hand, the threats to security in our democratic societies both necessarily determine the outcome of the balancing of security and privacy. To illustrate this: in Digital Rights Ireland and Seitlinger, the Court considered the importance and ubiquitous nature of electronic communications and connectivity in our information society. Possibly, after the Charlie Hebdo attacks, threats to the security of States and individuals will play a bigger role in the balancing by the Court. This may influence the outcome of the balancing process.

\textsuperscript{1311} Case C-362/14, Schrems, EU:C:2015:650, at 94.
\textsuperscript{1312} See Chapter 3, Section 7 of this study, distinguishing mass surveillance and targeted surveillance.
\textsuperscript{1313} See also: Frederik Zuiderveen Borgesius, Improving Privacy Protection in the area of Behavioural Targeting, Dissertation 2014, at 3.3.
\textsuperscript{1314} Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final.
Second, the ruling shows that it is not easy to balance both concerns in a meaningful way, in view of the difficulty of measuring the effects of an instrument on both concerns and to make comparisons. The Court did not base its ruling on evidence relating to the effectiveness of the instrument of data retention. The ruling is rather based on a theoretical reasoning that data retention “genuinely satisfies an objective of general interest”, but subsequently needs to be reviewed in the light of proportionality.

Third, the protection of fundamental rights should not depend on the political preferences of the day of a majoritarian body. We have seen that the Treaties underline the universal nature of these rights. However, practice shows that the actual state of a society determines what constitutes an intrusion. In the first decennium of this 21st century, we saw a relatively high legislative production for the protection of security relating to terrorist threats, post 9/11. These legislative measures were a reaction to threats that, also under the reasoning in Digital Rights Ireland and Settlinger, may be proportionate, but exceeded the scope of the actual threat, by widening the purpose of the measure and by not containing a time limit.

Fourth, the relation between privacy and security is not a trade-off between two incompatible values. Strong privacy and data protection – which implies, for instance, data security and data minimisation – can benefit law enforcement. The challenge is to include synergies in the decision-making.

18. **The CJEU also promotes Integration and acts as an Umpire where Other Public Interests or Other Governmental Actors have an Impact on the Exercise of Article 16(1) TFEU**

As explained in Section 3, the tasks of the Court of Justice of the European Union as a constitutional court do not only involve the protection of fundamental rights, but also include promoting integration, in particular of the markets, and acting as umpire between the various powers. In the context of Article 16 TFEU these functions are closely related. The Union’s competence under Article 16 TFEU has an impact on the competences of the Member States to protect other fundamental rights and public interests such as security.

An integrationist approach of the Court prevents Member States from deviating from the harmonised level of data protection, and, at the same time, means that the Member States are limited in the exercise of competences which compete with Article 16 TFEU. The function of integration may also prevent a Member State from requiring – in the national context – a

---

1316 Some evidence was available in the Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final. The author remembers that the evidence was intensively discussed during the oral hearing of the case, but this discussion was not reproduced in the ruling.

1317 At 44 of the ruling.

1318 This is a more general point that, e.g., plays a role as justification of the functioning of the independent data protection authorities.

1319 At 59 of the ruling explains clearly why, in the CJEU’s view, this is problematic.

level of data protection that is higher than the level of protection agreed for the European Union.

The Court of Justice also adjudicates – as umpire – on disputes on competences between the European institutions, which have nothing to do with integration. The dispute before the Court on passenger name records (PNR) between, on the one hand, the European Parliament and, on the other hand, the Commission and the Council on the occasion of the first PNR agreement between the EU and the US is an example of the latter. In this case, the European Parliament successfully challenged the competence of the Commission and the Council to enter into an agreement with the US on the transfer and use of passenger name records of air passengers, but not because the European Parliament disagreed that the subject matter should be dealt with at EU level.1321

**Market integration: an additional interest to be taken into account by the CJEU**

The function of market integration is important in data protection, if only because EU data protection law is also in the interest of the internal market. Recital (3) of Directive 95/46 emphasises the free flow of personal data. Although after the Lisbon Treaty the internal market component lost importance,1322 the reform of the legislative framework for data protection is closely linked to the creation of a digital single market,1323 which requires for instance a more coherent framework.1324 Market integration played a role in *ASNEF and FEMCED* where the European Court of Justice ruled that Member States did not have discretion to specify a specific provision of European data protection law, namely Article 7(f) of Directive 95/46. The Court referred to the impact of national data protection rules on the internal market, emphasising that the directive intends to ensure an equivalent level of data protection in all Member States.1325

The exercise of the rights to privacy and data protection influences other public interests. This is recognised in Directive 95/46 itself. The directive contains exemptions and restrictions for a wide, but exhaustively listed number of interests.1326 Moreover, the directive allows the processing of personal data if this is necessary for the performance of a task carried out in the public interest,1327 without specifying the public interests at stake. The use

---


1322: As explained in Chapter 7, Section 9, in relation to the CJEU’s case law on the independence of the data protection authorities.


1327: Article 7(e) of the Directive.
of these exemptions and restrictions – quite often at national level – does not only affect the level of fundamental rights protection but also EU integration.

By way of example we refer to the exemptions and restrictions on the harmonised level of data protection in relation to national concerns of public health. Public health is also mentioned in Article 36 TFEU, as a ground for justifying measures of Member States prohibiting or restricting the free movement of goods in the European Union. A high level of health protection is furthermore recognised under EU law in Article 168 TFEU and in Article 35 Charter as an objective to be pursued in all EU policies. Processing of personal data in the interest of a high level of health protection may take place in a great variety of situations, from prevention and the combat of serious cross-border health threats to medical research. A more targeted use of personal data may take place if this “is necessary in order to protect the vital interests of the data subject”, which, under Directive 95/46, is recognised as a ground for the lawful processing of personal data. Vital interests are closely related to the survival of the data subject. However, in the context of health protection quite often medical data of individuals are processed. They are special categories of data and, therefore, enjoy specific protection.

In short, public health is a complicated area, where national policies interact with the harmonised level of privacy and data protection under Article 16 TFEU. It exemplifies that the use of national competences for public interests, like health, adversely affects the level of integration reached under Article 16 TFEU. Market integration is an additional interest to be taken into account by the Court of Justice, where it rules on the basis of Article 16 TFEU, because of the close link between privacy and data protection and the digital single market.

The CJEU as an umpire between different powers: precise answers by the CJEU are required, where the CJEU adjudicates on Article 16 TFEU and relating competences

Article 16 TFEU impacts on other public interests, such as security, that may require exceptions or limitations to fundamental rights protection. Article 52(1) Charter allows limitations to fundamental rights such as the rights to privacy and data protection “if they are necessary and genuinely meet objectives of general interest recognised by the Union”. Article 52(1) Charter encompasses a wide range of interests, covering, for instance, the interests listed in Article 36 TFEU as possible exceptions of free movement under EU law. Article 52(1) does not contain an exhaustive list of interests, but it is defensible that the interests to which the Explanations refer must considered to be exhaustive, in the light of the general

1328 Article 35 Charter also establishes a fundamental right of access to preventive health care and the right to benefit from medical treatment, but that right is not directly relevant for the subject of this study.
1332 Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, on Article 52.
requirement to interpret limitations to fundamental rights restrictively. However, this exhaustive listing does not give much guidance, since the Explanations refer to a wide range of interests and objectives. Moreover, the example of public health shows that applying exceptions and limitations to data protection is complicated.

The restriction of the use of Article 52(1) Charter can, therefore, better be found in the test of the seriousness of the invoked public interest. In this respect, there is a similarity with the exceptions to free movement as developed in the case law of the Court of Justice on free movement under the rule of reason, opening the door for reasonable national measures restricting free movement.

Often, the competence of the European Union under Article 16 TFEU impacts on other competences of the the Union or the Member States. The absence of EU competence or the limits posed on EU competence by competing competences can be invoked by EU institutions or by the Member States. This interaction between the Union and the Member States – which is most relevant for this study – is related to managing centralisation, an inherent effect of the exercise of the Union’s mandate under Article 16 TFEU, in connection with the competences of the Member States.

The Court of Justice deals with the interaction with the Member States in a direct manner, when the Union’s competence is challenged by a Member State because of the absence of a sound legal basis, but also in more indirect ways in preliminary procedures. An important parameter for measuring how the Court deals with the discretionary powers of Member States is its preciseness in the answering of preliminary questions. It may apply a “doctrine of deference” leaving national judges discretion in solving the cases or it may take an approach based on integration and hierarchy, solving conflicts of law itself. A strong defender of a “doctrine of deference” is Gerards, who argues that leaving a wide margin of appreciation by the Court to national instances enhances the legitimacy of the European Union. However,

---


1335 An example in data protection is: Joined cases C-317/04 and C-318/04, European Parliament v Council (C-317/04) and Commission (C-318/04), EU:C:2006:346. In this case the European Parliament challenged successfully the EU competence to conclude an agreement with the US on the transfer of use of passenger name records of air passengers. Summary in: Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 308.

1336 This subject is mainly addressed in respect of the contributions of the legislator and of the DPAs.

1337 Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010, at 7-009 to 7-012 (and the cases mentioned there). In data protection, Case C-301/06, Ireland v Parliament and Council, EU:C:2009:68.


she accepts that a clear and serious impairment of a central objective of the Treaties justifies an intensified judicial review.

Above we argued that effectively protecting privacy and data protection requires that the Court of Justice answers preliminary questions in a precise manner. Precise answers are also important where the Court adjudicates on the competences under Article 16 TFEU and relating competences. The contrary view would prejudice a harmonised and effective privacy and data protection, under the rule of law.

19. Conclusions

The judicial review of the fundamental rights to privacy and data protection by the Court of Justice of the European Union is essential in making the Union’s mandate under Article 16(1) TFEU work. The Court of Justice fulfils its role, for instance, by systematically interpreting Directive 95/46 in the light of Articles 7 and 8 Charter. The extensive role of the Court compensates to a certain extent for the democratic deficit of the Union. Where the EU structures do not provide for satisfactory democratic control on the EU institutions and structures, individuals enjoy judicial protection, ultimately guaranteed by the Court.

The Court of Justice must deal with the remarkable features of Article 16 TFEU and Article 8 Charter. As an example, the interpretation of the right to data protection under Article 8(2) Charter draws on the acquis laid down in Directive 95/46. This reasoning is circular, since the Court interprets Directive 95/46 in the light of the Articles 7 and 8 Charter. (Section 2)

The Court of Justice does not just interpret the law by solving the disputes brought before it or by answering preliminary questions of national courts. In the exercise of its tasks, the Court also acts as a constitutional court with three functions: the review of fundamental rights, market integration and umpire between the various powers. The – perceived – activist role the Court plays qualifies it as a suitable actor for privacy and data protection on the internet. The preliminary ruling procedure is a success, also in the field of privacy and data protection. However, the case law of the Court is by definition incremental. The Court cannot develop a comprehensive policy for better protection. (Section 3)

As explained, the extensive role of the Court of Justice compensates for the democratic deficit of the European Union, yet the Court has further legitimacy because of its close link with national courts, in particular through the preliminary ruling procedure. It enhances its legitimacy by properly balancing the interest of EU integration and national interests. The Court gives guidance, by adjudicating in cases interpreting EU data protection legislation in the light of Articles 7 and 8 Charter. Guidance by the Court is not sufficient for bridging the gap between general principles and practice; other mechanisms are also needed. (Section 4)

Until the Lisbon Treaty, the Court of Justice referred to fundamental rights as principles under Member States’ law and took account of the European Convention on Human Rights. The Court ruled itself on possible infringements of fundamental rights, as part of its task of
ensuring a uniform interpretation of EU law. Over the years, the importance of fundamental rights increased in the case law, but Articles 7 and 8 Charter were only mentioned once. (Section 5)

The entry into force of the Lisbon Treaty prompted the Court of Justice to fundamentally change its approach in relation to fundamental rights. The Court’s assessment of limitations of a fundamental right focuses on proportionality. The Charter has become the yardstick and has a wide scope, but with limits. (Section 6)

The test under the Charter is stringent, depending on a number of factors. The nature of the fundamental right is such a factor. This factor is analysed in more detail in this study, focusing on the question whether meaningful distinctions can be made between fundamental rights, in order to improve the protection of the most essential rights on the internet. (Section 7)

Various methods of defining fundamental rights are useful for understanding fundamental rights: a positive method, a method based on the nature of the right and a method based on the historical background. All three methods have advantages in understanding privacy and data protection in relation to other fundamental rights. (Section 8)

The Charter does not establish any hierarchy between fundamental rights. This study proposes a simple taxonomy enabling a difference in the standard of review for fundamental rights protection on the internet, without creating a hierarchy. This taxonomy has a number of purposes. Thus, it should prevent any weakening of privacy and data protection (and other fundamental rights that are most crucial for our democracies), resulting from the equal protection of all rights. In addition, it should assist in compensating for the particular challenges of certain rights on the internet, and enable an efficient use of resources. Finally, it would allow a focus on extraterritorial application of fundamental rights, taking into consideration legitimate claims of third countries or international organisations. (Section 9)

The study suggests that the legitimacy of the Court’s role would further improve were the Court to assess the application of the rights to privacy and data protection, taking this simple taxonomy into account. Privacy and data protection fall within the second category of fundamental rights, with a high impact on human dignity. This means more concretely: (1) there is a necessity of protection in an online environment; (2) where needed, extraterritorial application of the rights must be safeguarded; (3) the rights should be applicable in horizontal relations; (4) restrictions and limitations of these rights are subject to a strict test; (5) where a balance is needed with other fundamental rights and public interests, the essential nature of the rights to privacy and data protection should be taken into account; and (6) this may lead to an approach where the Court adjudicates itself, and does not defer the matter to the national courts (in preliminary ruling procedures). These requirements are in line with the strict approach the Court already takes on privacy and data protection. (Section 10)

The case law of the US Supreme Court differs from that of the EU Court of Justice in respect of the balancing with free speech. It is therefore not surprising that Google Spain and Google
Inc. was heavily criticised in the US, because of its presumed impact on free speech. However, where privacy and data protection need to be balanced with the public interest of security, there is synergy with the approach of the US Supreme Court. Both Courts contributed to the legal development in relation to privacy and data protection in law enforcement, by taking account of the intrusive consequences of the information society. For instance, the US Supreme Court decided that, generally, a warrant is needed for searching a smartphone. (Section 11)

The link between the fundamental rights of privacy and data protection, on the one hand, and freedom of expression and information, on the other hand, is changing and intensifying due to internet related developments. The dividing line between private and public speech is becoming blurred, changes are caused by the impact of a free and open internet, and new intermediaries, like search engines, play a role in promoting freedom. The debate on the right to be forgotten demonstrates that, where an individual is entitled to request deletion of personal data, this automatically impacts on the right to receive information under Article 11 Charter. (Section 12)

In Google Spain and Google Inc., the European Court of Justice takes into consideration the changed reality in the information society, which has an impact on privacy and data protection and on the balancing between fundamental rights. The ubiquitous availability of information implies a lack of control on the part of the data subjects and potentially restricts their autonomy. The Court no longer takes a deferential approach and gives search engines a social responsibility, giving them the task of balancing between fundamental rights, a task close to the core tasks of government. (Section 13)

The right of access to documents gives effect to core values in society such as transparency and democratic control. The Court of Justice scrutinises strictly, but not where balancing is needed with privacy and data protection. Applicants invoking transparency must demonstrate the necessity of having access to documents if these documents include personal data. The Court does not seem to balance privacy and data protection on an equal footing with public access to documents. (Section 14)

There are different scholarly views on the status of the right to property as an essential value in a democratic society. The right to property is not included in all fundamental rights treaties. The enforcement of intellectual property is becoming more complex in the information society and copyright is the example of a right which is difficult to enforce. However, if intellectual property is balanced against privacy and data protection on an equal footing, this may weaken the level of data protection, resulting from accepting internet monitoring of individuals by copyright holders. (Section 15)

The relationship between privacy and data protection and security has elements of a trade-off. Privacy is, on the one hand, seen as inhibiting the appropriate protection of our societies against threats caused by terrorist attacks or by serious crime, yet, on the other hand, it is considered a value that should prevail against risks of unconditioned surveillance. The Court of Justice builds on the case law of the European Court of Human Rights on privacy and
security, which includes a strict review of measures that aim at creating a high level of security, but have an impact on privacy and data protection. (Section 16)

*Digital Rights Ireland and Seitlinger* gives indications for balancing privacy and security. First, the outcome is determined by trends in these two areas, the ubiquitous connectivity and the security threats for society. Second, objectively measuring the effects of a legislative instrument and making comparisons is not easy. Third, a lack of transparency characterises government surveillance. Fourth, privacy should not depend on political preferences of a majoritarian body. Fifth, strong privacy and data protection can benefit law enforcement. The challenge is to find synergies. (Section 17)

The Court of Justice of the European Union also promotes market integration and acts as an umpire where other public interests or other governmental actors impact on the exercise of Article 16(1) TFEU. The integration of the Union in general and of EU markets in particular is an additional interest to be taken into account by the Court, where it rules on the basis of Article 16 TFEU. Moreover, insofar as the Court acts as an umpire between various powers, precise answers by the Court are required, particularly where it adjudicates on the competences under Article 16 TFEU and relating competences. (Section 18)

This chapter outlined the contribution of the Court of Justice of the European Union to the mandate under Article 16 TFEU. A taxonomy of fundamental rights has been proposed, as a specific tool for further improving the level of protection. This taxonomy divides fundamental rights into the following categories: (1) non-derogable or absolute fundamental rights, corresponding to the rights included in Title I of the Charter, entitled ‘dignity’; (2) the rights with a huge impact on human dignity, but not qualified as non-derogable; and (3) the social, cultural and economic rights. Further categories include: principles in the Charter (as meant in Articles 51(1) and 52(5) thereof); the fundamental freedoms of the Treaties, relating to free movement; and the undefined species of public and general interests.
Chapter 6. Understanding the Scope and Limits of the EU Legislator’s Contribution to the Mandate under Article 16 TFEU

1. Introduction

The right to data protection as a claim based on fairness requires safeguards where personal data are processed. These safeguards are primarily laid down in legislative acts. The Treaty on the Functioning of the European Union empowers the EU legislator – the European Parliament and the Council – to adopt rules on data protection. These rules must ensure that individuals can effectively enjoy their right to data protection.

This chapter analyses the contribution of the EU legislator, an element of the research question which is specified as: “what does and should the European Union do to make Article 16 TFEU work, through legislation?” This analysis includes the following subjects:

a. the general design of the contribution;
b. the institutional role of the legislator, the contributions of the EU institutions, as well as the involvement of other stakeholders in the legislative process;
c. a short comparison with the mandate of the EU legislator on equal treatment and non-discrimination;
d. the areas in which the Members States should exercise competence;
e. the interfaces with other competences of the EU and the Member States;
f. the conditions for good legislation and for engaging the private sector, with a key role for the concept of accountability.

The first objective of the chapter is to understand the scope and the limits of the contribution of the EU legislator to the mandate under Article 16 TFEU, in relation to the role of competences of the Member States. The second objective is to assess the choice of instruments by the EU legislator, against the complex reality of an information society that threatens privacy and data protection and that leads to a perception of loss of control.

Article 16(2) TFEU lays down that the European Parliament and the Council, in their common capacity as EU legislator, have the duty to adopt the rules on data protection and, therefore, it must be seen as an explicit choice of the TFEU to bring data protection legislation to the Union level. The use of the definite article ‘the’ may give the impression that the EU legislator is the exclusive legislator within the Union on data protection and that, consequently, there shall be no national legislation in this domain. However, the Member States exercise – and should exercise – competence for certain elements of the protection of privacy and personal data, particularly in order to provide legitimate and effective protection of these rights.
The EU legislator is not only confronted with competing competences, but has an even greater concern: EU rules must ensure data protection against the background of an information society that threatens privacy and data protection and also leads to a perception of loss of control. The EU legislator should choose the proper instruments to ensure privacy and data protection, for instance by focusing on the accountability of data controllers.

Section 2 discusses the general design of the legislator’s contribution, whereas Sections 3 and 4 analyse the contributions of the various partners in the legislative process. Besides the institutional partners (the European Parliament, the Council and the Commission), these also include the Member States and the private sector and civil society.

Section 5 makes a short comparison with the mandate of the EU legislator under Articles 18 and 19 TFEU on equal treatment and non-discrimination, noting three differences. Section 6 identifies elements of privacy and data protection in respect of which the Member States should exercise competence.

Sections 7 and 8 deal with the interfaces between privacy and data protection, on the one hand, and the competences of the European Union and its Member States in related areas, on the other hand. The Member States are competent to deal with rights and interests other than data protection. Also where the Union itself has competences in other areas, this may have an impact on the mandate of the EU in the field of data protection. The areas discussed are the freedom of expression and information, the right of access to documents, intellectual property and the public interest of security. Sections 9-11 analyse synergies with public interests relating to the internal market: the economic dimension of privacy and data protection. Specific areas where synergies exist are electronic communications, consumer protection and competition law. All these Sections 7-11 are complementary to the interconnection between data protection and other fundamental rights and public interests under the case law of the Court of Justice of the European Union as discussed in Chapter 5.

The second objective of this chapter, assessing the choice of instruments by the EU legislator against the background of the information society, is the subject of Sections 12-14. Section 12 briefly discusses the privacy rules in the United States, as an introduction to multi-stakeholder approaches. Section 13 shows that effectiveness of protection on the internet requires engaging the private sector. Section 14 forwards accountability as a solution for delivering privacy and data protection. Section 15 presents this chapter’s conclusions.

2. A General Design of the Legislator’s Contribution: What needs to be done?

Article 16(2) first sentence TFEU reads: “The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.”
This provision grants a legal basis for EU legislation in the area of data protection. It is widely formulated and gives the European Union the opportunity to deliver upon its ambitions. Article 16 applies to all processing activities taking place within the scope of EU law, with one exception: specific rules will be adopted by the Council for the Common Foreign and Security Policy, under Article 39 TEU.  

The scope of the mandate: Article 16(2) TFEU contains a duty to adopt EU legislation

The mandate under Article 16 TFEU extends to the rules relating to data protection, with regard to the processing of personal data by the EU institutions and bodies, the authorities of the Member States and the private sector.

The first sentence of Article 16(2) TFEU gives the EU legislator a tool to actively ensure privacy and data protection. The question arises whether this tool imposes on the EU legislator an obligation to act. In general, the power of EU institutions to adopt legislative acts is not considered to be a duty, but there are exceptions. The issue is whether Article 16(2) TFEU can be considered as such an exception and whether this legal basis obliges the European Union to legislate in this area. These may seem to be purely academic questions given that EU data protection law already exists, with Directive 95/46 as the main instrument, and given the pending reform of the legislative framework. However, Directive 95/46 only covers the former first pillar of the EU Treaty and in the former third pillar the EU rules are incomplete. There is no guarantee that the reform of the EU framework for data protection – once fully adopted – will cover all areas where personal data are processed and will ensure the control by independent authorities in all these areas.

Moreover, in view of the perceived loss of control in the information society, legislation is indispensable to ensure the individual has a right which has meaning in practice. Under the principle of subsidiarity this must be EU legislation, in view of the scale of the problem, but in accordance with that same principle of subsidiarity the Member States have an important

---

1340 The final sentence of Article 16 TFEU reads: “The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union. “ Article 39 does not play a significant role in practice and is not specifically addressed in this study. See also Chapter 4, Section 2.
1344 The former third pillar covers police and judicial cooperation in criminal matters. As explained in Chapter 4, Section 3, there are no general EU rules applicable to purely national situations; Article 1(2) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.
role to play within the pluralist legal context of the European Union.\(^{1345}\) Furthermore, in exercising its legislative mandate, the Union must ensure that the rules are effective.\(^{1346}\) The legislator must take conditions of quality of legislation into consideration, to ensure that the protection is indeed effective.

Article 16(2) TFEU states that the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, \textit{shall} lay down the rules on data protection. This provision is precisely formulated, its scope is wide and, in principle, not subject to conditions.

This formula also means that the material scope of the rules must include all personal data and that any exception to the material scope cannot be laid down in secondary EU law. An illustration of this situation is provided by amendments proposed by the European Parliament in the legislative procedure of the General Data Protection Regulation, aiming at excluding ‘pseudonomysed data’ from the scope of protection. However, pseudonomysed data by definition relate to an individual and cannot be taken out of the scope of protection, since they are personal data.\(^{1347}\) As Barak explains, in the theory on fundamental rights a distinction is made between the boundaries of a fundamental right (”scope” or “\textit{Normbereich}”) and the extent of protection. The limitations imposed by legislation can only affect the protection given by a fundamental right, not its scope. This is relevant for this study because, under this theory, EU law does not allow the legislator to limit the scope of the data protection under Article 8 Charter.\(^{1349}\)

The European Union shall lay down \textit{the} rules. In itself, this formula does not give sufficient grounds to qualify the assignment of Article 16(2) TFEU as an obligation. Other provisions in the Treaties are formulated in a similar manner, providing that the European Parliament and the Council \textit{shall} lay down \textit{the} rules. An example is the legal basis for the internal market in Article 114 TFEU.

However, not only is the wording of Article 16(2) TFEU precise, but legislation is also needed to give practical meaning to the right to data protection. These two arguments substantiate the view that Article 16(2) TFEU does indeed impose an obligation on the EU legislator. The classical case in this respect is \textit{European Parliament v Council}\(^{1350}\) of 1985, on the European transport policy. In this case, the European Court of Justice accepted that there was an obligation to act by the legislator (at the time the Council, the European Parliament not yet having legislative powers), because the obligation to act was sufficiently well-defined.

\(^{1345}\) See Chapter 4, Section 4 of this study.

\(^{1346}\) As discussed in Chapter 4, Section 15.


\(^{1348}\) Aharon Barak, Proportionality; Constitutional Rights and their limitations, Cambridge University Press 2012, e.g. at 19-26.

\(^{1349}\) Possibly, the ‘household exception’ in Article 3(2) of Directive 95/46 could be seen as a limitation of the scope; see: Case C-212/13, Ryneš, EU:C:2014:2428, and the case note by H. Hijmans: On Private Persons Monitoring the Public Space C-212/13, in EDPL, 2015/2.

taking into account that the result to be achieved was determined by the EC Treaty. The EC Treaty also included a time limit for the legislator.\textsuperscript{1351} The obligation of the EU legislator to act under Article 16(2) TFEU could be established on the basis of this reasoning of the Court of Justice although, admittedly, a time limit is not included in Article 16(2) TFEU.

The result to be achieved is determined by Article 16(1) TFEU: the right of everyone to data protection would not be meaningful if there were no legislation defining the main substance of the right and ensuring control by independent authorities. To conclude, if Article 16(2) TFEU would indeed impose an obligation on the EU legislator, non-compliance with this obligation could successfully be challenged before the Court of Justice as a failure to act.

This study defends the view that Article 16(2) TFEU, first sentence, raises the expectation that the rules adopted by the EU legislator cover the whole domain of data protection, notwithstanding the fact that not all the rules in the area of data protection should be laid down at EU level. The data protection reform – with the General Data Protection Regulation as the centrepiece – should lead to the full implementation of this duty of the EU legislator, also in areas where at present EU rules are lacking.\textsuperscript{1352}

\textit{The mandate of the EU legislator has two remarkable features}

The mandate of the EU legislator is neither unrestricted nor exhaustive. The legislator must take into account conditions set in other areas of EU law or, in other words, other mandates of national legislators and the EU legislator. This is the logical sequel of the interfaces between data protection and other fundamental rights and public interests as recognised in the case law of the Court of Justice of the European Union.\textsuperscript{1353} Besides, data protection legislation itself serves different interests. It is not solely adopted for the protection of the fundamental rights of individuals, but it also has an economic component, which is to ensure the free flow of information. These considerations restrict the discretion of the EU legislator in the exercise of its task.

A closer look at Article 16(2) TFEU, first sentence, reveals two incoherences in the text. First, although the provision gives effect to a fundamental right under the Charter, it is also formulated as covering the rules relating to the free movement of such data. The added value of the reference to free movement is not evident. One could argue that the reference to the free movement of data is mainly a remnant from the past and in particular from one of the two objectives of Directive 95/46, providing that “personal data should be able to flow freely from one Member State to another”.\textsuperscript{1354} The relevance of this objective is underlined by the Court of Justice,\textsuperscript{1355} but seems less important after the entry into force of the Lisbon Treaty,\textsuperscript{1351} In (the former) Article 75 of the EC Treaty.

\textsuperscript{1352} Such as the processing of personal data within the police and judicial sectors, in the absence of cross-border elements; see Chapter 4, Section 3.

\textsuperscript{1353} As explained in Chapter 5.

\textsuperscript{1354} Recital (3) of the directive.

\textsuperscript{1355} Most recently in Case C-362/14, Schrems, EU:C:2015:650.
now data protection is recognised as fundamental right under EU law. In our view, the EU legislator is not required to lay down a separate set of rules on the free flow of information.

It is safe to say that the addition in the text of the free movement of personal data does not change much, as far as the material scope of Article 16(2) TFEU, first sentence, is concerned. It does however have a meaning for the personal scope of this provision. By common interpretation, Article 16(2) TFEU does not only apply to activities of the EU institutions and the authorities of the Member States, but also to activities of the private sector. This is most clearly evidenced by the fact that Directive 95/46 applies equally to the public and the private sectors and that the General Data Protection Regulation will apply to both sectors.

The second incoherence in the text of Article 16(2) TFEU is the limitation of the mandate, as far as processing of personal data by the Member States is concerned. The mandate only applies to the Member States when they carry out activities that fall within the scope of Union law. This limitation is not supposed to have a self-standing meaning. As explained in Chapter 5, it follows from the wide formulation of the right to data protection in Article 16(1) TFEU that all processing by Member States falls by definition within the scope of EU law.

What about the competence of the Member States?

As explained in Chapter 4, this is an area where the European Union shares competence with the Member States. Data protection is not mentioned in any of the exhaustive lists on exclusive, respectively supporting, coordinating and complementing competences, included in Articles 3 and 6 TFEU. Although data protection is equally not included in the open list of shared competences of Article 4 TFEU, it is a shared competence, precisely because the latter list is open. Member States may only act to the extent the Union has not exercised its competence.

Although Article 16(2) TFEU is qualified as a shared competence, there is not much autonomous room for the Member States to adopt legislation in this area, in view of the scope and nature of the mandate of the EU legislator under Article 16(2) TFEU, as explained above. Moreover, under the principle of subsidiarity, protection can – normally – better be achieved by EU action than by the Member States acting individually, in view of the scale and effects of the action. This is the particular consequence of the fact that on the internet all acts, in principle, have a cross-border effect. In short, the mandate of the EU legislature is a complete mandate, leaving little autonomous room for the Member States, particularly after the entry into force of the General Data Protection Regulation, which will take away most of the Member States’ autonomy.

---

1357 In Section 2.
1359 This is the wording of the principle of subsidiarity in Article 5(3) TEU.
However, this is only part of the story. The Member States remain an essential player in this area. Privacy and data protection as guaranteed by EU law have an impact on core competences of Member States and, therefore, the Member States also have a legitimate role to play, although often by delegation.

First, data protection is a sensitive subject area affecting the daily lives of the citizens. In the field of privacy and data protection, competences are attributed to the EU level, but Member States retain a responsibility for protecting the fundamental rights of their citizens.

Second, a role of the Member States also results from the effect of data protection law on core government tasks such as the protection of other fundamental rights and ensuring the physical security of the citizens.

Third, Member States play a role, because of the European Union’s organisational structure – leaving implementation and enforcement to a large extent in the hands of the Member States – and as a result of the limitation of EU power under Article 4(2) TEU, particularly on national security.\textsuperscript{1360}

Fourth, the legislative framework on data protection under Article 16 TFEU interferes with an even wider range of areas of public interest. All personal data processing in the public sector (and the private sector as well) must be based on one of the legitimate grounds mentioned in Article 7 of Directive 95/46. Hence, data protection has a cross-cutting effect on all policy areas where personal data are processed. This means, virtually all areas of government intervention, also in policy areas where the Union has no or limited competences.

All in all, the EU legislator operates in a complex reality

The complex reality is evidenced by the developments in connection with the General Data Protection Regulation. The European Union acts internally within a pluralist legal context, with an important role for the Member States in accordance with the principle of subsidiarity. On the one hand, as the Commission’s analysis of subsidiarity illustrates,\textsuperscript{1361} the General Data Protection Regulation is supposed to strengthen the role of the Union in an area where a developed EU legal framework already exists, namely in Directive 95/46 and other legal instruments. On the other hand, there are multiple claims of Member States, with an impact on data protection legislation under Article 16(2) TFEU, first sentence. The complex reality is illustrated by the difficult negotiations on the General Data Protection Regulation over a period of several years.\textsuperscript{1362}

\textsuperscript{1360} This was explained in Chapter 4.
\textsuperscript{1361} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final, Explanatory Memorandum, at 3.2.
\textsuperscript{1362} See Chapter 10, Section 10 of this study.
3. The EU Legislator’s Institutional Role, Institutional Balance and the Contributions of the European Parliament, the Council and the Commission

Under the ordinary legislative procedure as defined in Article 294 TFEU, a legislative act is adopted jointly by the European Parliament and the Council on a proposal from the Commission. This procedure has become the rule under EU law.\footnote{Koen Lenaerts and Piet van Nuffel, There are exceptions in the Treaties, not relevant here. See: European Union Law, Third edition, Sweet & Maxwell 2010, at 16-004.} The involvement of these three institutions must ensure the legitimacy of the legislative procedure and hence of EU action, with the caveat being that the legitimacy of the European Union to act in the area of data protection is also influenced by the – presumed – democratic deficit of the Union.\footnote{See Chapter 4, Sections 8-11.} This section deals with the legislative process, under the ordinary legislative procedure.

The main actors in the legislative procedure are the Council and the European Parliament, as the two institutions endowed with legislative power, and the Commission, which has the monopoly of legislative initiative. An analysis of the roles generally taken on by the European Parliament, the Council and the European Commission in the legislative process exceeds the scope of this study. Nevertheless, this chapter includes remarks on the various roles in the legislative procedure, with specific relevance for the tasks under Article 16 TFEU. The outcome of the legislative process, bringing together the institutions’ different roles, has, by definition, the features of a compromise.

The legislative procedure is made more legitimate and effective by including other actors in the legislative process. These are representatives of the Member States, the private sector, civil society and expert bodies.

Finally, the ordinary legislative procedure does not provide for any formal role for the European Council, which is composed of the Member States’ heads of state and government. Sometimes, however, European Council conclusions support the legislative process. For example, conclusions of the European Council emphasised the need for the data protection reform and gave an impetus to the legislative process.\footnote{E.g., the Conclusions of the European Council of 24-25 October 2013, available on: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf.} This role of the European Council will not be discussed further.

*There is one EU legislator, but composed of three institutions*

Under the ordinary legislative procedure, the legislative power lies with the European Parliament and the Council. However, they cannot act of their own motion, without an initiative of the Commission. The monopoly of legislative initiative is established in Article 17(2) TEU. Both the European Parliament and the Council may request the Commission to
submit proposals. If the Commission does not give effect to such a request, it must motivate its decision.\textsuperscript{1366}

Despite the different responsibilities of the three institutions, the emphasis in practice is on compromise and dialogue,\textsuperscript{1367} as illustrated by the important role of the trilogues – not provided for in the Treaties – in the decision-making process.\textsuperscript{1368} This justifies speaking about one legislator, whilst at the same time recognising that, in the words of Craig: “The EU institutions have always been ‘singular’.\textsuperscript{1369}” The input of the three institutions, respecting the institutional balance, gives democratic legitimacy to the EU legislator’s mandate, with the nuances relating to the Union’s democratic legitimacy explained in Chapter 4.

However, the institutions each play their own role within the EU system, based on an institutional balance. The positions the institutions take on data protection and their input in the negotiations on the data protection reform also reflect institutional concerns. An example is the legislative resolution of the European Parliament of 11 February 2010.\textsuperscript{1370} In this resolution, the European Parliament withholds its consent to the conclusion of an agreement between the European Union and the United States on the Terrorist Finance Tracking Program. This legislative resolution was based on considerations of privacy and data protection, but was also a demonstration of Parliament’s newly acquired competences in the Lisbon Treaty that had just entered into force and gave the European Parliament binding powers in relation to this type of agreements.\textsuperscript{1371} A second example concerns the institutions’ positions in relation to delegated and implementing acts, foreseen in the proposed General Data Protection Regulation. Both the European Parliament and the Council were very critical of the high number of provisions empowering the Commission to adopt delegated and implementing acts.\textsuperscript{1372} The difference in position between the European Parliament and the Council, on the one hand, and the Commission, on the other hand, is presumably also based on institutional considerations.

\textit{The European Parliament as a supporter of strong privacy and data protection}

\textsuperscript{1366} This is laid down in Article 225 TFEU (European Parliament) and Article 241 TFEU (Council), which also includes the request for a study.
\textsuperscript{1367} Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 127-129.
\textsuperscript{1368} Raya Kardasheva, Trilogues in the EU legislature, King’s College London, Department of European and International Studies, Research Paper, 30 April 2012.
\textsuperscript{1369} Paul Craig in: Paul Craig and Grainne de Búrca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 41.
\textsuperscript{1370} European Parliament legislative resolution of 11 February 2010 on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (05305/1/2010 REV 1 – C7-0004/2010 – 2009/0190(NLE)).
\textsuperscript{1372} See on this in Dutch: H. Hijmans, De nieuwe Europese privacywetgeving: stand van zaken bijna twee jaar na Commissievoorstel, Nederlands tijdschrift voor Europees recht, 2013/10, at 349.
In the successive Treaty changes, the powers of the European Parliament have been strengthened in order to alleviate the Union’s democratic deficit and to better reflect the will of the people in the decision-making process. At the same time, national parliaments are more closely involved.1373

In the debates on the rights to privacy and data protection, the European Parliament has sought to play a role supporting the recognition and strengthening of these rights, although it was reported that more involvement of the European Parliament did not necessarily lead to a higher level of protection.1374

The approach of the European Parliament as a proponent of stronger privacy and data protection is illustrated by its long term involvement in the debates on public authorities’ access to personal data processed by the private sector.1375 As was indicated before, in 2010 the European Parliament used its newly acquired powers to reject the agreement with the United States on the Terrorist Finance Tracking Program. The agreement was finally adopted, taking into account the objections of the European Parliament that had led to the initial rejection.1376 After the Snowden revelations in 2013, the European Parliament called for the suspension of the agreement.1377

A second occasion where the European Parliament was systematically involved was the dossier on passenger name records (PNR) that related to public authorities’ access to reservations of passengers, mostly with airlines. In this dossier, the European Parliament played an active role in opposing, at various instances, to agreements with the United States and other third countries,1378 and was also very critical of using PNR for law enforcement within the European Union. In April 2013 the Civil Liberties committee of the European Parliament rejected the Commission Proposal for a directive on the use of passenger name record data (EU PNR).1379

---

1373 Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 57-58. See also Chapter 4, Section 10.
1377 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance.
In the debates on the reform of the European data protection framework, the European Parliament takes a leading role, emphasising both the urgency for reform and the need for robust data protection. An illustration of the latter is the way the European Parliament deals with the proposal for a directive on data protection in the area of law enforcement. First, it insists on the need for considering this proposal as part of a package, together with the proposed General Data Protection Regulation, so as to avoid that the two eventually will be separated, which may lead to long delays for the directive on data protection in the area of law enforcement. Second, the European Parliament proposed amendments with specific obligations for law enforcement authorities dealing with personal data, in addition to the general data protection principles.

**The Council of the European Union representing national concerns**

In general, the role of the Council is the representation of national interests. However, it is also an EU institution that takes part in the decision-making process. As Craig & de Búrca explain, it represents a mix of intergovernmental and supranational interests.

The reform of the European data protection framework has proved to be a long and difficult process in the Council, even though the heads of government in the European Council – the highest political level in the EU – have underlined the reform’s importance. National concerns complicated progress being made in the adoption of the proposal. These concerns related, for instance, to the impact of the proposed regulation – aimed at replacing national laws on data protection – on existing provisions in various national laws containing specific data protection safeguards.

---

1381 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final.
1382 The proposed directive suffered from resistance within Council, relating to the fact that Member States are reluctant in accepting wide involvement of the EU in the police and justice sectors.
1383 European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)), amendments relating to Articles 4-19.
1385 Conclusions of the European Council 24-25 October 2013, at 8: “It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework [...] is essential for the completion of the Digital Single Market by 2015.”
Another constant factor in the Council is the impact of EU data protection law on security, a core competence of the Member States. This is a reason why, for instance, the proposal for a directive on data protection in the area of law enforcement was not given the same priority as the proposed General Data Protection Regulation.\textsuperscript{1388}

\textit{The European Commission, committed to integration}

Whereas the Treaty on European Union describes the tasks of the European Parliament and the Council in terms of powers, it only gives an orientation for the Commission. Pursuant to Article 17 TEU the Commission shall promote the general interest of the Union. And indeed, in practice the Commission is seen as the political force most committed to integration.\textsuperscript{1389}

In its formal role of proposing legislation, the Commission enables the EU legislator to adopt rules and during the legislative process it acts as an – informal – broker between the European Parliament and the Council.

The delegated and implementing acts provided for in Articles 290 and 291 TFEU are a means for the Commission to remain influential after a legislative act has been adopted, by amending or supplementing non-essential elements of the act or by adopting uniform conditions for its implementation. These procedures replace the old structures for delegation, known as comitology-procedures,\textsuperscript{1390} and are a way for the Commission to act as legislator, subject to scrutiny by the Council and the European Parliament.\textsuperscript{1391} The procedures have been criticised because they lack democratic content.\textsuperscript{1392}

The justification of the proposal for a General Data Protection Regulation is illustrative for the Commission’s role. The comprehensiveness of the European data protection framework is a major impetus for the proposal, as is revealed by the title of the communication paving its way: “A comprehensive approach on personal data protection in the European Union”.\textsuperscript{1393} One of the main concerns leading to the proposal was the existence of differences in the

\textsuperscript{1387} Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.
\textsuperscript{1388} As illustrated by the fact the Council adopted a general approach (Note from Presidency to Council, 11 June 2015, 9565/15) in June 2015, but not yet for the Directive.
\textsuperscript{1389} Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 40.
\textsuperscript{1392} Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 150.
\textsuperscript{1393} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010), 609 final.
implementation of the existing EU data protection framework in the Member States. In other words, the reform is inspired by the preference for EU integration.

This does not mean that a preference for integration necessarily means more integration in all areas. The Commission is well aware that the EU legislator should not be involved in every issue in the European Union. As the Juncker Commission underlines in its endeavours for better regulation, the EU legislator should focus on big issues that cannot be solved by Member States alone. This focus is a continuation of Commission policy since the beginning of the 21st century.

4. Involving Other Stakeholders: Member States, Private Sector and Civil Society

This study emphasises the involvement of the Member States and of the private sector – and to a lesser extent of civil society – in the exercise of the EU mandate under Article 16 TFEU. This involvement is not only crucial in the application of EU law, but also in the legislative procedure. An important part of this procedure is the wide consultation of stakeholders during the process. The proposed General Data Protection Regulation illustrates the role wide consultations play. The proposal was presented as the result of consultations that lasted for more than two years and included a wide range of interested parties, and of an impact assessment. These interested parties included experts and expert bodies, as well as interested individuals. After the Commission adopted the proposal, these various interest groups continued to be involved. Albrecht, the rapporteur in the European Parliament, underlines for instance that many of the more than 4000 proposals for amendments in the European Parliament were instigated by the private sector.

The Commission’s communication on better regulation of 2015 emphasises the importance of consulting stakeholders in a wider manner. The Juncker Commission promises to consult more and listen better.

Involvement of actors within the Member States takes various forms

---

1395 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation for better results - An EU agenda, COM(2015) 215 final, p.3.
Although it is the Council’s role to reflect national interests in the EU legislative procedure, in addition, actors within the Member States representing national interests are involved through various other mechanisms.

At various stages of EU integration the Member States have claimed to retain competences in cases where the outcome of the legislative process would not reflect their preferences.\(^{1400}\) An example in current EU law is Article 114(4) TFEU that allows Member States, under strict conditions, to maintain national provisions on grounds of major needs after laws have been harmonised. More and more it is considered that the national government’s involvement in the Council is not enough and that other stakeholders at national level should also be involved.

Presently, the Treaties provide for national parliaments to be involved in the legislative procedure of the European Union. National parliaments have a right to show the ‘yellow card’\(^{1401}\) when they consider that the principle of subsidiarity has not been respected. This involvement should ensure that national preferences are taken into account and fits within the general assignment in Article 12 TEU for national parliaments to contribute actively to the good functioning of the Union. Furthermore, consultation of regional and local authorities represented in the Committee of the Regions\(^{1402}\) aims at enhancing the legitimacy of EU legislation in the various regions within the Union.

Member States’ interests are also put forward in various informal configurations, by interest groups with a national background or through the involvement of national experts and civil servants in policy-making.\(^{1403}\) The consultation of independent data protection authorities, as currently required under Article 28(2) of Directive 95/46, constitutes a separate type of consultation, aiming at obtaining specialised input from national experts. This expert advice should enhance the quality of EU legislation and hence increase its legitimacy and effectiveness. Chapter 7 addresses expert advice in relation to the legitimacy of these authorities themselves.

*Involvement of the private sector and civil society*

A broad consultation of stakeholders is part of the legislative process. Put in the wording of Article 11(2) TEU, the institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society.\(^{1404}\) As part of the legislative procedure the

---


\(^{1401}\) Protocol (No 2) on the application of the principles of subsidiarity and proportionality, annexed to the TEU and TFEU. Further read: Davor Jančić, 2015, “The game of cards: National parliaments in the EU and the future of the early warning mechanism and the political dialogue”, CMLR 52 (2015), 939–975. See also Chapter 4, Section 4.

\(^{1402}\) Article 300(3) TEU.

\(^{1403}\) Paul Craig and Grainne de Búrca, *EU Law, Text, Cases and Material*, Fifth Edition, Oxford University Press 2011, at 147, mentioning administrative interaction and the interlocking of bureaucracies at national and EU level.

\(^{1404}\) As required by Article 11(3) TEU.
Economic and Social Committee, consisting of representatives of employers and employees and of other parties representative of civil society, is consulted as well.\textsuperscript{1405}

Protocol No. 2 on the application of the principles of subsidiarity and proportionality annexed to the Lisbon Treaty states: “before proposing legislative acts, the Commission shall consult widely”. The consultation of stakeholders by the Commission is governed by a set of general principles, including participation (meaning an inclusive approach by consulting as widely as possible), openness and accountability.\textsuperscript{1406}

Involvement of the private sector and of civil society in the legislative process is an element of the Union’s governance method, reflecting what Craig describes as challenging state-centric views of governance.\textsuperscript{1407}

What do we learn, in relation to tasks, limitations, legitimacy and effectiveness?

The involvement of these different stakeholders in the decision-making process must give the procedure further democratic legitimacy. The objective of this involvement is to reach an outcome that takes account of the different interests at stake, or the different spheres involved in the European process, as van Middelaar calls them.\textsuperscript{1408} These spheres include the interests of EU citizens, of Member States and of integration. Integration as a result of Article 16 TFEU is not a goal in itself but an instrument for internet privacy and data protection, which includes the bureaucratic capacity to deliver and aspires to public acceptance of EU involvement.

\textbf{5. A Comparison with the Similar, but not Equal Mandate of the EU Legislator under Articles 18 and 19 TFEU on Equal Treatment and Non-Discrimination}

The EU legislator’s mandate under Article 16 TFEU has to a certain extent a specific character within the EU Treaty framework applicable to fundamental rights. Although Article 16 TFEU relates to core competences within a democratic society, it is generally formulated as a wide assignment to protect the fundamental right of data protection, without specific limits. It is a mandate of an unconditional nature, giving effect to a fundamental right, both at the EU level and within the Member States. Comparable mandates relating to fundamental rights are more limited. For example, the EU legislator’s mandate to adopt rules under Article 15 TFEU on access to documents is limited to documents of the EU institutions, bodies, offices and agencies.

\textsuperscript{1405} Article 300(2) TFEU.
\textsuperscript{1408} Luuk van Middelaar, De passage naar Europa. Geschiedenis van een begin (published in English as: The Passage to Europe: How a Continent Became a Union), Historische Uitgeverij.
The EU legislator’s competences which are most similar to its mandate under Article 16(2) TFEU are laid down in Article 18 TFEU dealing with non-discrimination on grounds of nationality and Article 19 TFEU on the combat of discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Article 18 and 19 TFEU correspond to the fundamental right enshrined in Article 21 Charter. The grounds for discrimination in Article 19 TFEU are enumerated more specifically in Article 21 Charter. This study does not envisage any elaborate comparison of data protection with the area of equal treatment and non-discrimination, an area where a vast acquis of case law and EU legislation exists. However, the similarities have provoked some observations that may be helpful for a better understanding of the EU legislator’s mandate under Article 16(2) TFEU.

Articles 18 and 19 TFEU are similar to Article 16 TFEU because they deal with a fundamental right and provide for a competence of the EU legislator to adopt rules in relation to this fundamental right. Another similarity is that non-discrimination developed under EU law in the same way as data protection, from an instrument for the internal market to a fundamental right. However, there is also an important difference. Whereas Article 16 TFEU provides that the Council and the European Parliament shall adopt the rules on data protection, the provisions on equal treatment and non-discrimination state that the EU legislator may adopt rules (Article 18) or take appropriate action (Article 19) which includes legislation. Hence, the wording of Articles 18 and 19 TFEU leaves more discretion to the Member States.

There is a similarity in the nature of the EU legislator’s competence. In both domains the EU legislator has an impact on citizens’ daily lives in that it deals with fundamental rights, in which, additionally, ethical considerations, such as human dignity, play an increasing role. Bell describes this as a process of constitutionalisation, where an existing norm is entrenched in a constitutional framework and accorded a higher legal status. The similarity with EU data protection is obvious. Whereas data protection was regulated under Directive 95/46 with an internal market legal basis, it is presently grounded in primary law, with the status of a fundamental right.

---

1410 Articles 18 and 19 TFEU are not formulated as fundamental rights, but must be understood as such, in line with Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, on Article 21.
1412 As follows from Article 19(1) TFEU read in combination with Article 19(2) TFEU.
1413 Examples can be found in the developments with respect to discrimination on the ground of sex, Mark Bell in: Paul Craig and Grainne de Burca, The evolution of EU Law, Second Edition, Oxford University Press 2011, at 614-618.
This has two consequences. First, high standards of effective protection are observed, due to this increased status. *Test-Achats*\(^{1415}\) is the example in the area of non-discrimination. In this case, the European Court of Justice overruled a derogation within an instrument of EU law because this derogation did not comply with the Charter. Hence, the Court delimits the EU legislator’s discretion to adopt derogations from a fundamental right. This approach demonstrates that inclusion of a right in the Charter raises the fundamental rights standard. This finding concurs with the assessment of limitations to the exercise of a fundamental right under Article 52(1) Charter, which is particularly strict.\(^{1416}\) It also concurs with the test under EU data protection law, as illustrated by the recent case law on data protection, in particular *Digital Rights Ireland and Seitzinger*\(^{1417}\) and *Google Spain and Google Inc.*\(^{1418}\). However, the lesson from *Test-Achats*\(^{1419}\) is that the EU legislator should formulate the exceptions and limitations to the right to data protection in a precise manner, not exceeding the necessity for an exception or limitation to protect a specific, public, interest.

Second, the Member States may claim discretionary powers precisely because the constitutional nature of fundamental rights protection gives legitimacy to Member States’ action. The protection of fundamental rights is part of the core of national sovereignty.\(^{1420}\) In this context, too, there is a parallel with non-discrimination and equal treatment. The Member States retain a discretionary power for giving additional protection to weaker categories of persons through positive discrimination, in addition to EU law leading to harmonisation. Without going into details, positive discrimination by Member States is allowed to combat sex-based discrimination, but within limits.\(^{1421}\)

The question arises whether a similar approach could be envisaged for data protection, or whether the wording of Article 16 TFEU would prohibit legislative measures providing for additional protection by Member States, unless explicitly foreseen in a legislative instrument of the European Union on data protection. This study takes the position that, under Article 16 TFEU, these discretionary powers do not exist and so additional legislative measures by Member States, designed to complement Directive 95/46 or – in the future – the General Data Protection Regulation, are not allowed unless explicitly provided for. This position is in line with the Court’s ruling in *ASNEF and FECEMD*\(^{1422}\) on the direct effect of Article 7(f) of Directive 95/46. Further arguments are the difference in wording between Article 16 TFEU on the one hand and Articles 18 and 19 TFEU on the other hand, combined with the fact that the harmonisation of EU data protection law is not only in the interest of the internal market but also serves to ensure a high and uniform level of data protection in the digital single

\(^{1415}\) Case C-236/09, Association Belge des Consommateurs Test-Achats, EU:C:2011:100.

\(^{1416}\) As explained in Chapter 5, Section 6.

\(^{1417}\) Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitzinger (C-594/12), EU:C:2014:238.

\(^{1418}\) Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.

\(^{1419}\) Case C-236/09, Association Belge des Consommateurs Test-Achats, EU:C:2011:100.

\(^{1420}\) See on this more extensively, Chapter 4, Section 8, of this study.


\(^{1422}\) Joined cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777. See also Chapter 5, Section 3.
market,\textsuperscript{1423} which is particularly important in an internet environment. However, this position is not evident in the absence of case law of the European Court of Justice. A more nuanced approach is not excluded, for instance in the public sector where the link with the internal market is less obvious.

6. **Elements of Privacy and Data Protection where Member States should exercise Competence: Five Categories**

As has been explained above, the rules adopted under Article 16 TFEU should cover the whole area of data protection. A closer look at the proposed reform package\textsuperscript{1424} shows that the two legislative proposals the Commission submitted in 2012 cover most of the area of data protection, although the proposals exclude the data processing by EU institutions and bodies.\textsuperscript{1425}

The proposed General Data Protection Regulation also illustrates that national law under Article 16 TFEU remains relevant, even in the area that will be covered by the regulation, after its entry into force. This proposal shows that the Member States should have a role to play when there is an interface between the mandate of the EU legislator and the competences of the Member States in related areas. In his Opinion on the regulation, the European Data Protection Supervisor\textsuperscript{1426} distinguished four categories of provisions where the Member States should exercise competence in privacy and data protection.

These categories are: provisions where EU law builds on national law because national law provides a ground for processing personal data, for instance in the public interest; provisions where EU law mandates national law to give effect to its provisions, for instance where EU law obliges the Member States to establish data protection authorities; provisions where EU law allows or requires national law to specify EU rules; and provisions where EU law allows or requires national law to depart from EU rules. This distinction is used as the basis of this section and expanded with a fifth category.

The first category results directly from Article 8 Charter, which provides that data processing must be based on the consent of the person concerned or have some other legitimate basis

\textsuperscript{1423} E.g., to prevent forum shopping by data controllers choosing the forum where the level of protection is perceived to be low; see Chapter 8, Sections 3 and 5.

\textsuperscript{1424} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final; Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.

\textsuperscript{1425} Article 2 of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. This article contains more exceptions, which are related to the scope of EU law (national security) and to the scope of the rules in Article 16 TFEU itself (the rules in the area of the Common Foreign and Security Policy are adopted on another legal basis, namely Article 39 TEU). The ‘household exception’ (Article 2(2)(d) of the proposal) was the subject of of Case C-212/13, Ryneš, EU:C:2014:2428.

\textsuperscript{1426} European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at II.2.a.
laid down by law. In the latter case, the legal ground for processing may be based on EU or national law, as is made explicit in Article 6(3) of the proposed General Data Protection Regulation. This ground is of particular interest in the public sector. Public authorities process personal data in many policy domains in the public interest or in order to fulfil a legal obligation, without consent given by the data subject. Hence, in the terminology of Article 8 Charter, processing of personal data in the public sector is, in many instances, based on a legitimate basis laid down in law, and not on consent. National law determines that data processing is allowed and EU law, based on Article 16 TFEU, lays down the conditions. The situation becomes more complicated when the national law refines the conditions under EU law, which may interfere with the direct effect of EU law.

The second category covers situations where the national law builds on and gives effect to EU law. Certain provisions of the proposed General Data Protection Regulation may require implementation. An example is the obligation of Member States to set up independent data protection authorities. Chapter VI of the proposed regulation illustrates that EU law determines that the Member States assign public authorities with the task of ensuring control of EU data protection law and determines conditions for the establishment and functioning of these authorities. The specific position of these authorities in the national legal framework will be determined by national law. It follows from the principle of national procedural autonomy, explained in Chapter 4, that not all aspects of the establishment and functioning of the national data protection authorities will be laid down in EU law.

The third category relates to provisions mandating or allowing the Member States to specify an EU regulation. This is the situation meant in Article 2(2) TFEU where the European Union has exercised its competence and thereby has a blocking effect on the competences of the Member States. The Member States may only legislate where this is explicitly mandated or allowed by a provision of EU law. Such a specific provision of EU law may leave room to the Member States in order to respect the cultural differences and cultural diversity between the Member States or the national identities, but also for other reasons. Examples of such specific provisions can be found in Articles 80, 81, 82, 84 and 85 of the proposed General Data Protection Regulation. These relate to freedom of expression, health, employment, professional secrecy and churches and religious associations.

The fourth category of exercising national competences in EU data protection consists of the exceptions and derogations to EU data protection law, which are in many instances left to

---

1427 Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final: “The basis of the processing […] must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject.”
1428 This was the case – under Directive 95/46 – in Joined cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777, where the Spanish law refined Article 7(f) of the Directive, contradicting EU law.
1429 Articles 46-50 (and recitals 92-96) of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. These articles are fairly specific on these authorities. See further Chapter 7.
1430 As explained in Chapter 4, Section 3.
1431 As recognised in Article 167(4) TFEU and explained in Chapter 4, Section 5.
1432 Article 4(2) TEU, as explained in Chapter 4, Section 5.
national law. This is logical since – as is illustrated by Article 13 of Directive 95/46 – exceptions and derogations to the exercise of the right to data protection are often related to core state functions, such as national security and the combating of crime. Since this category consists of exceptions and derogations of fundamental rights under EU law, the scope of these exceptions must necessarily be interpreted strictly. As explained in Chapter 5, with references to the case law of the Court of Justice of the European Union, the test under the Charter is strict, with high requirements as to the proportionality of measures interfering with the rights to privacy and data protection. This strict proportionality test, paradoxically, is also a justification for leaving the exceptions and derogations within the remit of the Member States. Member States can be more precise in limiting the scope of exceptions and limitations to situations where this exception or limitation is necessary and proportionate in view of the specific public interests they pursue.

This leads to considering a fifth category, which was not specified in the Opinion of the European Data Protection Supervisor on the reform package. This category concerns provisions enabling the Member States to balance privacy and data protection with other fundamental rights, in areas where the competence to legislate lies primarily or entirely with the Member States. As explained by Barak, this balancing is of a different nature than the scrutiny of exceptions and derogations to privacy and data protection. A national law could deal with the conflict between privacy and data protection and another fundamental right under Member States’ competence. An example is a provision under national law specifying the conditions of access to documents of the national administration containing personal data. In this situation the Member States have discretionary power. However, such a provision should not delimit the validity or the scope of the right to data protection, as a fundamental right in the Charter.

7. The EU Legislator’s Mandate and its Interfaces with Competences of the EU and the Member States in Related Areas

The mandate of the EU legislator under Article 16(2) TFEU, first sentence, to lay down the rules on data protection is not unrestricted. The EU legislator is – in the exercise of its mandate – confronted with interfacing competences of the European Union itself and the Member States, in related areas. These interfaces have an impact on the mandate under Article 16 TFEU. However, the EU legislator must under all circumstances remain in a

---

1434 And the more or less corresponding Article 21 of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
1435 As illustrated by Case C-236/09, Association Belge des Consommateurs Test-Achats, EU:C:2011:100.
1436 E.g., with reference to Joined cases C-92/09 and C-93/09, Schecke (C-92/09) and Eifert (C-93/09) v Land Hessen, EU:C:2010:662 and to Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
1437 European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at II.2.a.
position to exercise its competences under Article 16 TFEU in an effective and legitimate manner.

These interfacing competences influence the exercise of the EU legislator’s mandate in different ways. They may delimit the mandate, because a balancing is required between privacy and data protection, on the one hand, and competing competences in related areas, on the other hand, for instance relating to the protection of other fundamental rights or security. Yet, they may create synergies with privacy and data protection, for instance because EU competences in the internal market aim at creating trust in the information society, which concurs with an objective of data protection. These competences may also be instrumental to enhancing privacy and data protection, by creating synergies in enforcement.

The interfaces with other competences affect the EU legislator’s scope of action under Article 16 TFEU. In addition, where the other competences belong to the Member States, dealing with an interface also influences the division of competences between the Union and the Member States. Strengthening privacy and data protection – in contrast with other fundamental rights and essential interests – also implies, in principle, a centralisation of competences at EU level.

*Freedom of expression and information: an area where the EU only has limited competence, but where developments in the information society have a big effect*

Under the Treaties, there is no general competence for the European Union to adopt legislation that aims at ensuring the effective protection of the freedom of expression. This is logical for three reasons. First, freedom of expression is an area where – as a rule – the State needs to abstain rather than take positive action. An exception is the active obligation resulting from Article 11(2) Charter to ensure freedom and pluralism of the media. Second, it is an area where Member States have retained their sovereignty for a number of reasons linked to their national identities and where limitations to the freedom of expression have an important cultural and historical component. The prohibition in Germany of the dissemination and use of propaganda by unconstitutional and National Socialist organisations is an example of the latter. Third, the media are mostly territorially fragmented within the Member States of the Union.

---


1441 E.g., the German Penal Code contains a section on “Threats to the Democratic Constitutional State” (§§ 84 to 91). This section “contains provisions forbidding the dissemination and use of propaganda by unconstitutional and National Socialist organizations”, Winfried Brugger, The Treatment of Hate Speech in German Constitutional Law (Part I), German Law Journal, Vol. 4, No. 1 (1 January 2003), at 16.

1442 This is changing, as e.g. recognised by AG Cruz Villalón in his opinion in Joined cases C-509/09 and C-161/10, eDate Advertising and Martinez, EU:C:2011:192.
However, the European Union has a role when EU measures in other areas touch upon the freedom of expression or when Member States’ actions falling within the scope of EU law affect the freedom of expression. Directive 2000/31 on electronic commerce exempts internet service providers from liability and prohibits them from being subject to a general monitoring obligation. These provisions strengthen the freedom of expression.\footnote{1443} An example of an EU law which includes limits to the freedom of expression and which is relevant for this study, is the Directive 2010/13 on audiovisual media services.\footnote{1444} This directive is applicable to certain internet services and contains provisions that prohibit content that includes any incitement to hatred based on race, sex, religion or nationality or that seriously impairs the physical, mental or moral development of minors.

The exercise of the freedom of expression is significantly affected by the developments in the information society. The European Court of Human Rights has underlined this on various occasions, by stating: “In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the sharing and dissemination of information generally.”\footnote{1445} At the same time, a free internet and Web 2.0 allowing every individual to upload content have significantly extended the possibilities of individuals to exercise their rights, and at the same time reduced their dependency on traditional media. The internet has also diminished the territorial fragmentation of the information landscape.\footnote{1446}

Obviously, these in themselves positive developments also increase the risks of undesired effects of the freedom of expression. The wide possibilities for expression enable hate speech, can cause harm for minors, or lead to defamation or a breach of privacy of individuals. These risks relate to the amount of personal data that is diffused and also to the fact that responsibilities are more dispersed. In many situations, there is no longer one obvious data controller.

The derogation for journalistic purposes under Article 9 of Directive 95/46 expresses the close connection of the freedom of expression and information with the rights to privacy and data protection. This derogation will be broader under Article 80 of the proposed General Data Protection Regulation, allowing Member States to reconcile the right to protection of personal data with the rules governing freedom of expression.\footnote{1447} However, the General Data Protection Regulation does not give the Member States any guidance to ensure that they balance the fundamental rights on an equal footing.

\footnote{1444} Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ L 95/1.
\footnote{1445} E.g., \textit{Times Newspapers Ltd v the United Kingdom} (Nos 1 and 2), Nos 3002/03 and 23676/03, § 27, ECHR 2009
\footnote{1446} See Chapter 2, Section 8 of this study.
Open data and the interface between transparency and data protection

The developments in the information society affect the transparency of governments in a significant manner. Notably, publication of government documents on the internet makes governments much more widely accessible than publication in a traditional register, which is still provided for in Regulation 1049/2001 on public access.1448 A more fundamental change is that governments apply the concept of open data.

Open data is a policy concept with basically two rationales: on the one hand, improving transparency and accountability of governments and, on the other hand, supporting innovation and economic prosperity, by giving open access to, mostly large, datasets of the government for reuse free of charge and copyright.1449 Open data corresponds to the idea that a broad use of data – and in particular data of public organisations – boosts the information economy, or in other words: “Documents produced by public sector bodies […] constitute a vast, diverse and valuable pool of resources that can benefit the knowledge economy.”1450 Older and illustrative examples of open data are found, for instance, in the United States where meteorological data and the global positioning system (GPS) were made freely available by the federal government, enabling the development by the market of all kinds of new tools and services.1451

Although the concept of open data was developed outside the scope of Article 42 Charter and Article 15 TFEU, also because of its economic purpose, it does give an impetus to the right of access to documents, since governments themselves are supposed to be committed to actively publish information. This could also strengthen claims by individuals in case this commitment is not followed in practice. Moreover, under the open data schemes, individuals do not only have a right of access to information, they also have the right to reuse the information.1452 Furthermore, under EU law individuals now also have a claim vis-à-vis Member States in respect of the documents they hold.1453

Open data is neither limited to nor focused on personal data, but of course in many occasions personal data are involved, and thus the rights to privacy and data protection are triggered. As

---

1449 Source: http://en.wikipedia.org/wiki/Open_data; see also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Open data, An engine for innovation, growth and transparent governance, COM(2011) 882 final. The introduction of this communication also mentions the participation of citizens in political and social life.
the European Data Protection Supervisor explains, open data may increase the risks of misuse of personal data, for instance if the data are reused for illegal or disproportionate purposes. Open data takes accessibility to a new level, by making entire databases available for reuse.\textsuperscript{1454}

Legislative measures for internet monitoring with the aim of enforcing intellectual property rights

Chapter 5 explained the case of \textit{Scarlet Extended}\textsuperscript{1455} on a filtering mechanism designed to monitor internet users. Internet monitoring requires a balancing between privacy and data protection, on the one hand, and intellectual property rights, on the other hand. This issue has also arisen as a result of acts of legislation. The ‘three strikes approach’\textsuperscript{1456} is an example of a new tool that led to controversy, \textit{inter alia} because of its impact on the rights to privacy and data protection. This was a legislative tool for the monitoring of internet users to combat illegal downloading, which in some cases could even lead to the disconnection of internet users. In essence, after two warnings a national authority could require an internet service provider to suspend internet access for the offending internet connection of an individual.

Also in the Anti-Counterfeiting Trade Agreement (ACTA),\textsuperscript{1457} which was rejected by the European Parliament on 4 July 2012,\textsuperscript{1458} these kinds of mechanisms were included as crucial means for the enforcement of intellectual property mechanisms. The agreement allowed schemes enabling copyright holders to monitor internet users and to identify alleged copyright infringers.\textsuperscript{1459} The intense political discussions on ACTA focused on the effects on fundamental rights, including the freedom of expression and information.\textsuperscript{1460}

\section*{8. Security: An Area where the EU and the Member States have Significant Competence

\begin{itemize}
\item \textsuperscript{1454} European Data Protection Supervisor, Opinion of 18 April 2012, the ‘Open-Data Package’ of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), at 2.2.
\item \textsuperscript{1455} Case C-70/10, \textit{Scarlet Extended}, EU:C:2011:771.
\item \textsuperscript{1456} See on the ‘three strikes approach’: European Data Protection Supervisor, Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ C 147/1. A good example is France, where a law created a government agency called \textit{Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet} (HADOPI), with as one of its tasks the application of the three strikes approach. The law was declared unconstitutional by the \textit{Conseil Constitutionnel} (Décision n° 2009-580 of 10 June 2009) and later abrogated, but not because it infringed privacy. See on the relationship between data protection abnd intellectual property also Chapter 5, Section 15.
\item \textsuperscript{1457} The final text is available on: \url{http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf}. See in particular Article 27.
\item \textsuperscript{1459} Article 27 of ACTA does not prescribe those schemes, but allows them. See on this: European Data Protection Supervisor, Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ C 147/1, at IV.2.
\item \textsuperscript{1460} See on this: \url{http://freeknowledge.eu/acta-a-global-threat-to-freedoms-open-letter}.
\end{itemize}
The European Union’s exercise of its legislative competence on the basis of Article 16 TFEU may have an impact on core State functions, such as the protection of physical security. To a certain extent, the relation with security is addressed in Declaration (20) on Article 16 TFEU – dealing with national security although this is not mentioned in the title of the declaration – and Declaration (21) on the protection of personal data in the fields of judicial cooperation in criminal matters, and police cooperation.\textsuperscript{1461}

However, the interfaces of security with privacy and data protection are much wider, also because the protection of security is a priority for both the European Union and the Member States. As the European Council concludes, it is essential to guarantee a genuine area of security for European citizens.\textsuperscript{1462} As a result, the legislative debate is often dominated by demands of law enforcement agencies to allow a wide use of personal data. These demands are \textit{inter alia} based on the claim that technology using personal data makes law enforcement more effective. Hence, laws are adopted allowing wider use of personal data for security purposes. Conversely, the judicial debate is dominated by considerations of effective protection of privacy, on the acceptable level of intrusion. The follow-up of \textit{Digital Rights Ireland and Seitlinger}\textsuperscript{1463} is an example of these trends.\textsuperscript{1464}

The Treaty of Rome of 1957 recognised public security as one of the grounds allowing Member States to derogate from the free movement provisions in the EEC Treaty. These derogations are now included in, for instance, Article 36 TFEU (relating to free movement of goods), Article 52 (relating to the freedom of establishment) and Article 62 (relating to the free movement of services). In the case law of the European Court of Justice, public security extends to both internal and external security.\textsuperscript{1465} Equally, EU directives for the harmonisation of the internal market contain provisions on possible derogations by Member States from the harmonisation pursued by the directives for reasons of public security. Examples are Article 3(4) of Directive 2000/31 on electronic commerce,\textsuperscript{1466} which also mentions national security and defence, and Article 16(3) of Directive 2006/123 on service in the internal market.\textsuperscript{1467} In the area of data protection, Article 13 of Directive 95/46 contains wide possibilities for Member States to restrict the scope of the obligations and rights laid down in the directive, mainly for reasons of public security. The text of Article 13 additionally refers to national security, defence and the combat of crime.\textsuperscript{1468}

\textsuperscript{1461} See also Chapter 2, Section 10 of this study.
\textsuperscript{1463} Joined cases C-293/12 and C-594/12, \textit{Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)}, EU:C:2014:238
\textsuperscript{1468} And a number of other ground, not relevant in this context.
Whereas safeguarding public security was at first left to the Member States and not considered to be a task of the European Union, this changed with the inclusion in 1992 by the Maastricht Treaty, of an area of freedom, security and justice in the Treaties. This area is established for the purpose of ensuring the safety and security of the peoples, originally as a flanking measure of the free movement of persons. However, this limited rationale was gradually replaced by a wider assignment. As the first multi-annual programme in the area of freedom, security and justice (Tampere, 1999) specified: “People have the right to expect the Union to address the threat to their freedom and legal rights posed by serious crime.”

The Lisbon Treaty made a further step towards developing an area of freedom, security and justice as one of the Union’s main building blocks. The pillar structure of the European Union disappeared and the area has now been fully integrated into the Treaty on the Functioning of the European Union and is no longer subject to specific procedures. The area is meant to facilitate the free movement of persons, while ensuring the safety and security of the peoples. In the TFEU, the task of providing security is specified in Article 67(3): “The Union shall endeavour to ensure a high level of security.”

The task of providing security under EU law must not only respect the Charter of Fundamental Rights of the European Union, but must also be exercised in respect of national sovereignty. Providing security as a core task of the state means that in the area of freedom, security and justice – an area of shared competence under Article 4 TFEU – only limited competences have been transferred to EU level, with the following nuance. First, Article 67(3) TFEU also refers to measures to prevent and combat crime (and xenophobia and racism) which may be an indication of the competence being broader. Second, the qualification of the Union’s competences as being either narrow or broad depends on the perspective that is adopted, for instance, whether the EU competence on security is compared to the internal market competences or to the situation before the Lisbon Treaty entered into force. Not all authors characterise the competences as narrow.

The EU competences have a wide impact on data protection and they also interconnect with the competences of the Member States. The role of the European Union focuses on the coordination and cooperation for reasons of security. This includes the exchange of large

---

1469 See recitals of the TEU.
1472 Despite the fact that there are significant exceptions to this rule.
1473 As laid down in the preamble of the TEU.
1474 Article 67(3) TFEU is included in Title V on the area of freedom, security and justice, and encompasses, strictly speaking, the internal security of the EU. However, internal and external security are closely connected. The wording “endeavour to ensure a high level of security” is also included in Article 67(3) TFEU.
amounts of personal data\textsuperscript{1476} between police and judicial authorities on the national and EU levels.\textsuperscript{1477} This exchange of information, including personal data, is a significant manifestation of coordination and cooperation between the Union and its Member States. This is well illustrated by the multi-annual programmes in the area of freedom, security and justice. The Hague programme of 2004\textsuperscript{1478} aimed at improving the exchange of information under the ‘availability principle’, which was meant to govern law enforcement related data exchange, whereas in the Stockholm programme of 2009\textsuperscript{1479} the Information Management Strategy for EU internal security was set out as one of the main orientations.

Beyond the internal EU instruments dealing with security and privacy much has also been done to ensure protection of individuals in the European Union within the international context, in particular where information was needed for the purpose of security in the United States or in connection with security issues shared between the EU and its Member States and the US.\textsuperscript{1480} The agreements on passenger name records (PNR) and on the Terrorist Finance Tracking Programme (TFTP) are the most obvious examples. Both agreements aim at balancing security and privacy.\textsuperscript{1481}

9. Synergies with Public Interests relating to the Internal Market: The Economic Dimension of Privacy and Data Protection

This section introduces synergies between the fundamental rights of privacy and data protection, on the one hand, and one of the European Union’s objectives, establishing and ensuring the functioning of an internal market,\textsuperscript{1482} on the other hand. The relation between these fundamental rights and the interests of the internal market is not by definition synergetic. Privacy is often perceived as having a negative impact on economic innovation, or as conflicting with new technology. For example, the PCAST Report, addressed to President Obama, puts the conflict between privacy and new technology centre stage.\textsuperscript{1483}


\textsuperscript{1477} For instance involving Europol and Eurojust.

\textsuperscript{1478} Council, The Hague Programme: strengthening freedom, security and justice in the European Union, OJ 2005, C 53/01, at 2.1. The ‘availability principle’ means that information available in one Member State for police purposes should also be available for colleagues in another Member State.


\textsuperscript{1480} Not exclusively, also other third countries require data on EU citizens. Examples are the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Records, signed on 25 June 2014, and the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, OJ L 186/4.

\textsuperscript{1481} These agreements will be further discussed in Chapter 9, Section 13 of this study.

\textsuperscript{1482} Wording taken from Article 26 TFEU. Pursuant to Article 3(3) TEU, the Union shall establish an internal market.

\textsuperscript{1483} Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology (PCAST Report), May 2014.
The recognition under EU law of privacy and data protection as fundamental rights, combined with the EU legislator’s mandate under Article 16(2) TFEU may adversely affect innovation and competitiveness of industries. This is the logical consequence of the role these fundamental rights play under EU law. Fundamental rights must be respected and Article 52 Charter requires that limiting the exercise of a fundamental right must be necessary and genuinely meet the objective of general interest.

The Charter does not exclude a limitation of a fundamental right in the economic interest. The Explanations to Article 52 Charter refer for instance to Article 3 TEU, which mentions economic growth and a highly competitive social market economy as part of the internal market. However, allowing economic interests to limit a fundamental right is criticised and under Article 8 ECHR the limitation is restricted to the economic well-being of a country as a whole, which does not include the interests of companies. Where economic growth and a highly competitive social market economy are invoked as ground for a limitation of the rights to privacy and data protection the threshold is high, also as a result of Article 52(3) Charter, which specifies that the meaning and scope of fundamental rights shall be the same as those laid down by the European Convention on Human Rights. More generally, it would be difficult to accept limitations to fundamental rights representing essential values in a democratic society for purely economic objectives.

Not conflicting, but interfacing and creating synergies

Another perspective for looking at the interface between privacy and data protection on the one hand and the internal market on the other hand is the – strong – economic dimension of privacy and data protection. Delivering privacy and data protection may be in the economic interest of a company, for instance where the respect of high privacy and data protection standards is considered a competitive advantage. The concept of Privacy by Design, which enables combining strong privacy with technological innovation, illustrates this. Moreover, the right to data protection, as laid down in Directive 95/46 also has an economic objective.

Article 3(3) TEU entrusts the European Union – as part of its responsibility for the internal market – with the task of promoting scientific and technological advance. In its Europe 2020 Strategy, the Commission gave an outline of how it proposed to “turn the EU into a smart, sustainable and inclusive economy delivering high levels of employment, productivity and

1487 Included, under the heading of data protection by design or by default, as an obligation to implement the appropriate technological and organisational measures in Article 23 of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
1488 The free flow of information in recital (3) of the Directive. See also Chapter 4, Section 3.
social cohesion.” One priority is smart growth, the development of an economy based on knowledge and innovation, which includes a true single market for online content and services. The Digital Agenda for Europe is a concretisation of this strategy. In an economy based on knowledge and innovation, personal data have become an asset. Privacy and data protection are set to positively influence – or even boost – growth and innovation because protecting these rights creates trust.

This economic perspective was, from the outset, a motivation for the European Union and other governmental actors to get involved in privacy and data protection. It is illustrative in this light that Directive 95/46 was adopted under the internal market legal basis of the Treaties and that its object is not only to protect fundamental rights, but also to ensure the free flow of personal data between the Member States, as an element of the establishment and functioning of the internal market.

A harmonised level of protection – which in a Union based on values necessarily means a high level of protection – is a condition for the establishment and functioning of the internal market of personal data, and can also positively affect the global market. Moreover, privacy and data protection are also recognised as factors creating trust, which is needed for economic growth and scientific and technological advance. In its Communication on a Digital Agenda for Europe of 2010, the Commission underscores that a lack of trust hampers the digital economy and includes privacy concerns amongst the main reasons for it. Creating trust is one of the main driving forces behind the modernisation of the legal framework for data protection. In the United States this relationship seems to play an even

---


1490 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final.

1491 See Chapter 3, Section 6. Further read: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy".

1492 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final, at 2.1.3 and 2.3.

1493 Article 100a TEC, later renumbered to Article 95 TEC and now to Article 114 TFEU.


1496 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final, at 2.1.3 and 2.3. Privacy and data protection are amongst a range of issues addressed in the Communication.

1497 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European
more predominant role. The 2012 White House paper on consumer data privacy in a networked world has as its rationale that privacy protection is critical to maintaining consumer trust in networked technologies.\textsuperscript{1498} Furthermore, requirements of privacy and data protection could boost innovation, where those requirements incentivise the development of privacy-friendly technologies, as is illustrated by the already mentioned concept of Privacy by Design.

However, as indicated before: a high level of data protection is not necessarily perceived as being positive for the development of the information society. One of the main issues in the legislative process on the proposed General Data Protection Regulation relates to its – supposedly – burdensome nature and the high costs for the economy it is presumed to have. This perceived negative effect of the General Data Protection Regulation has an additional dimension in the era of big data, in which the increased possibilities to collect, use and analyse massive amounts of data, including personal data, have in itself become the trigger of innovation.\textsuperscript{1499} The European Council, too, underlines the importance of big data, cloud computing and open data as driving forces of the European digital economy.\textsuperscript{1500}

**Synergies between privacy and data protection and economic interests**

In short, there are important synergies between privacy and data protection on the one hand, and economic interests on the other hand. Addressing these synergies is primarily a task of the EU legislator and not of the Court of Justice of the European Union, which adjudicates when there are disputes, but not where synergies between different areas of intervention can be found. Using synergies in different areas of intervention by the Union and its Member States enhances the legitimacy of the EU legislator’s contribution under Article 16 TFEU.

Privacy and data protection are set to create trust, positively influencing – or even boosting – growth and innovation,\textsuperscript{1501} for instance in connection with the Digital Agenda for Europe. The concept of Privacy by Design contains an obligation to implement the appropriate technological and organisational measures and enables combining strong privacy and data protection with technological innovation. This concept is included in the proposed General Data Protection Regulation as an element of data controllers’ accountability.\textsuperscript{1502} It also illustrates that it is possible to create synergies between privacy and data protection and

---

\textsuperscript{1498} White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012, e.g., in the foreword.

\textsuperscript{1499} Examples can be found in: Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology, as well as in Big Data: A Revolution That Will Transform How We Live, Work, and Think, Viktor Mayer-Schönberger and Kenneth Cukier, 2013.


\textsuperscript{1501} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final, at 2.1.3 and 2.3.

economic interests. Privacy by Design has two objectives: it enhances trust in data protection, and it creates economic incentives. It should thus also be an instrument in economic policies of the European Union.

Moreover, the right to data protection itself provides for a system of checks and balances and allows processing of personal data so long as requirements of fairness and lawfulness are satisfied. Both Article 16 TFEU and Directive 95/46 contain references to the free flow of data, an economic consideration. Directive 95/46 permits a limitation of certain rights and obligations for important economic or financial interests of a Member State or the Union. It thus seems that the system of data protection allows flexibility.

10. Two Illustrations for Synergies: The Legal Frameworks for Electronic Communications and Consumer Protection

The EU legislator is active in various areas related to privacy and data protection. Both electronic communications and consumer protection are areas of EU intervention illustrating that synergies with EU action in the area of privacy and data protection can be found. Addressing these synergies is primarily a task of the EU legislator.

The legal framework for electronic communications does not only include a directive on privacy and electronic communications specifying Directive 95/46, but also contains other instruments that potentially support privacy and data protection. More specifically, the EU legal framework gives governments responsibility in the area of network governance, in contrast with the governance of the internet infrastructure, with little role for governments. Government responsibility in network governance could be used for enhancing control over the processing of personal data, provided that governments take considerations of privacy and data protection into account in the exercise of this responsibility.

In the field of consumer protection, an example of synergy is Directive 2005/29 on unfair commercial practices, which prohibits misleading omissions and requires transparency in business-to-consumer transactions. This directive in the field of consumer protection could also be used to require internet service providers to apply transparent privacy policies.

---


1504 Recital (3).


The legal framework for electronic communications makes governments responsible for network governance

The opening-up of the telecommunications market, which was long dominated by state monopolies, was the trigger for intensive EU intervention in a sector which is now more usually called electronic communications, but basically is the traditional telecommunications sector. This sector comprises electronic communications networks and electronic communications services. The ‘information society services’, generally speaking the services providing content, fall outside the sector’s scope. The same goes for the internet infrastructure.

The EU intervention is widely known as the ‘Telecoms Package’. A fundamental modification of this package took place in 2009, changing a number of legal instruments. In 2013, as part of the Digital Agenda for Europe, the Commission proposed an even more fundamental change to the framework, in its Proposal for a Regulation concerning the European single market for electronic communications.

One important objective of the Telecoms Package is creating the conditions for effective competition, which could not be achieved by general competition law, but needs ex ante regulatory obligations as provided for in Framework Directive 2002/21. The intervention also aims at achieving other public interests and gives individuals certain rights. Directive 2002/22 on universal service establishes the rights of end-users and defines, with regard to ensuring the provision of a universal service, the minimum set of services of a specified quality to which all end-users must have access at an affordable price. The Telecoms Package also includes Directive 2002/58 on privacy and electronic communications, which must ensure that the individual’s privacy receives specific protection in the electronic communications sector, supplementing the general regime for privacy and data protection.

1514 Article 1(2) of the directive states that it particularises and specifies the Directive 95/46 on data protection.
Various other issues in the Telecoms Package are relevant for this study. To start with, Framework Directive 2002/21 and Directive 2002/22 on universal service both promote net neutrality.\textsuperscript{1515} Furthermore, the security and integrity of networks and services should be ensured. Article 13a of Framework Directive 2002/21 requires that measures be taken ensuring a level of security appropriate to the risk presented. Network providers must also guarantee the integrity of their networks and thus ensure the continuity of the services supplied over those networks. Breaches of security and losses of integrity must be notified to the competent national regulatory authority. This obligation to notify is comparable to the personal data breach that must be notified to the national data protection authority under Article 4(3) of Directive 2002/58 on privacy and electronic communications. The relation between those two notifications is not fully clear. Combining these two notifications could strengthen protection, but could also lead to legal uncertainty. Finally, the providers of networks and services may be subject to a general authorisation\textsuperscript{1516} and in any event, they are under close scrutiny by a national regulatory authority.

The proposed regulation concerning the European single market for electronic communications has the ambitious goal to allow providers of electronic communications and services to provide their services throughout the European Union on the basis of one single EU authorisation.\textsuperscript{1517} Moreover, the proposal aims at significantly strengthening the rights of end-users, in particular to better address cross-border situations. Article 23 of the proposal includes a provision on net neutrality, basically by giving end-users the freedom to access and to distribute the information and content of their choice.\textsuperscript{1518} Providers shall not restrict this freedom by blocking or slowing down specific content.\textsuperscript{1519}

This all means that, within the scope of the legal framework for electronic communications, the European Union requires a level of networks and services governance that contrasts with the situation of the internet infrastructure, which is characterised by loose governance mainly outside the influence of governments. At first sight this legal framework provides better guarantees for the protection of the fundamental rights to privacy and data protection.


\textsuperscript{1518} Further read: Darren Read, Net neutrality and the EU electronic communications regulatory framework International Journal of Law and Information Technology Vol. 20 No. 1.

\textsuperscript{1519} Article 23(5) of the Commission proposal is more complicated, and allows for instance traffic management, but this is the essence.
Furthermore, national regulatory authorities, supported by the Body of European Regulators for Electronic Communications (BEREC), play a central role in the control of the EU legal framework for electronic communications. This enforcement mechanism will be described in Chapter 7 of this study. At this stage, we are only indicating possible synergies in enforcement between these regulatory authorities and the data protection authorities.

Consumer protection

The Treaty on the Functioning of the European Union provides for consumer protection to be an integrated part of other EU policies and activities (Article 12). The TFEU also includes a separate title on consumer protection, containing one article (Title XV, Article 169) specifying the main concerns of consumer protection, as well the instruments to address them. Article 114(3) TFEU requires a high level of consumer protection in relation to internal market instruments.

Consumer protection is also included in Article 38 Charter, which reads: “Union policies shall ensure a high level of consumer protection.” Arguably, Article 38 – read in combination with Articles 12, 114(3) and 169 TFEU – contains a fundamental right to consumer protection rather than just a principle as meant in Article 52(5) Charter. The argument that Article 38 Charter is a fundamental right finds support in Commission v Germany (Deposit Guarantee) where the European Court of Justice affirmed that there must be a high level of protection. It subsequently underlined that this does not mean harmonisation needs to take place at the standard of the most protective Member State. However, in practice, Article 38 Charter does not give much added value to the above mentioned articles in the TFEU.


1522 Article 12 TFEU: “Consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities.”

1523 To be complete, Article 169(3) and (4) specify procedure and the relation with national law, but are not relevant here.

1524 Arguably, Article 38 – read in combination with Articles 12, 114(3) and 169 TFEU contains a fundamental right to consumer protection rather than just a principle as meant in Article 52(5) Charter.


Consumer protection plays an important role in the Court of Justice’s case law on exceptions to the free movement of goods, in relation to restrictive measures of the Member States and their compatibility with EU law.  

The EU legislation in the area of consumer law contains a number of notions and requirements which are familiar to the area of privacy and data protection, such as fairness, consent and transparency. A good example is Directive 2005/29 on unfair commercial practices, which prohibits not only misleading actions, but also misleading omissions and by doing so requires transparency in business-to-consumer transactions. A misleading practice which is directly related to internet privacy and data protection is the offering of ‘free’ services on the internet where individuals pay with their personal data, the ‘two-sided business’ models of online service providers. The misleading omission, in the sense of consumer law, would be not informing individuals about the collection and use of their personal data, for instance for advertising purposes, or more widely the absence of an understandable privacy policy. Consumer law could potentially place a significant burden on a service provider on the internet, and at the same time strengthen the position of the data subject. Arguably, and more generally, consumer law could acquire an additional dimension on the internet, since the lack of transparency in the online world increases the likelihood of consumers being misled.

The relationship between privacy and data protection on the one hand and consumer protection on the other hand is an area that is relatively unexplored in the European Union, but it is a relationship where synergies are possible. As observed above, a number of notions which are used in both areas concur and breaches of privacy and data protection could at the same time amount to a breach of the right to consumer protection. Synergy could also be achieved through cooperation in enforcement. In the Union, national authorities are responsible for the enforcement of consumer protection rules. These authorities have a

---

1530 Notions included in Directive 95/46 and other legislative instruments in data protection, and reflected in Article 8(2) Charter.
1531 For other examples and further arguments, European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", at 3.3.
1533 As explained in Chapter 3, Section 6.
1534 See on this: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", at 4.3.2.
1535 See on this: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy.”
duty to cooperate with each other to ensure compliance with EU consumer rules, the smooth functioning of the internal market and the protection of consumers’ economic interests. This cooperation includes mutual assistance and the exchange of information and could possibly extend to cooperation with data protection authorities.

11. Competition Law, a Specific Challenge for Creating Synergies

The main instruments of EU competition law concern the control of anti-competitive agreements (Article 101 TFEU), the control of market power (Article 102 TFEU) and merger control (based on Regulation 139/2004). These instruments must be interpreted in the light of the principle of an open market economy with free competition, favouring an efficient allocation of resources, and must prevent businesses from distorting competition by prohibiting certain agreements between companies and combating abuse of dominant market positions. Three objectives of competition law are: first, efficiency, based on the economic theory that goods and products are most efficiently produced where there is competition, second, protection of consumers and smaller enterprises against strong economic powers, and third, a contribution to the internal market.

There is a specific reason why competition law is relevant in the context of this study: the information economy with its asymmetric structure and in which personal data have become an asset leads to companies acquiring market dominance, precisely because they accumulate large quantities of personal data. The best example is the ‘two-sided business’ model of online service providers that offer services for ‘free’, but let consumers pay with their personal data since they fund the free services by selling the data to advertising companies. If these providers have a dominant market position, this adversely affects competition and, at the same time, the privacy and data protection of individuals who lose control over their data, also because they do not have a real alternative. This is a reason why seeking synergies...

---

1539 This principle is laid down in Article 120 TFEU on economic policy, as well as in Article 127 TFEU on monetary policy. It is considered applicable to EU competition law (see: Koen Lenaerts and Piet van Nuffel, Third edition, Sweet & Maxwell 2010; and by analogy: Paul Craig and Grainne de Burca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, Chapter 26). The provisions on competition in Articles 101-106 TFEU do not contain similar principles.
1540 Articles 101-106 TFEU; they also restrict State Aid (not relevant here).
1541 In the case law of the CJEU: “Article 81 EC [now: 101 TFEU], like the other competition rules of the Treaty, is designed to protect not only the immediate interests of individual competitors or consumers but also to protect the structure of the market and thus competition as such.” Case C-8/08, T-Mobile Netherlands BV, KPN Mobile NV, Orange Nederland NV and Vodafone Libertel NV v Raad van bestuur van de Nederlandse Mededingingsautoriteit, EU:C:2009:343, at 38.
1542 Further read: European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy". See also Chapter 3, Section 6 of this study.
between privacy and data protection on the one hand and competition law on the other hand may be a promising path to follow.

The synergy between the two areas played a role in the merger between Google and DoubleClick, which lead to decisions by the European Commission\(^\text{1543}\) and the United States Federal Trade Commission. In its decision, the Commission addressed the market position of the merged company, because of the combination of personal information obtained by both merging companies, but came to the conclusion that competition would not be affected. In the US, it was in particular the dissenting statement of FTC Commissioner Jones Harbour that addressed the issue, highlighting amongst other things the nexus between privacy and competition.\(^\text{1544}\)

The European Commission has not issued many competition decisions in relation to the information economy.\(^\text{1545}\) At present, the Commission is conducting two investigations in antitrust cases against Google. In April 2015, the Commission sent a Statement of Objections to Google because of an alleged abuse of Google’s dominant position in general internet search which amounts to more than 90% of the EU market.\(^\text{1546}\) These cases do not explicitly deal with personal data, but a few observations can nevertheless be made in relation to the subject of this study.

The first observation relates to the definition of the relevant market, the first stage of a legal analysis in competition cases. This definition seems to be particularly complicated in an internet economy and may require a fundamental rethinking of market definitions. One reason is that market boundaries are continuously evolving.\(^\text{1547}\) A more fundamental reason, however, is given by Jones Harbour.\(^\text{1548}\) Market definitions are normally based on products or services. As she explains, in an economy based on big data\(^\text{1549}\) it makes more sense to define a product market for data, rather than a market based on specific uses of data by specific companies.

\(^{1543}\) Commission Decision, C(2008) 927 final, declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/DoubleClick).


\(^{1549}\) Obviously, this may not be in line with the requirement of purpose limitation under EU data protection law, but that is not the point we want to make here. On big data, see Chapter 3, Section 6 of this study.
The issue is that companies\(^{1550}\) collect large amounts of data that will later be sold or shared with others for purposes far beyond the purpose of initial collection and for purposes that are only defined in a later stage. This phenomenon is connected to the two-sided business model on the internet,\(^ {1551}\) where companies are active on different markets of products and services, and where – large amounts of – personal data are critical to both sides. Search engine providers are the example:\(^ {1552}\) the amount and quality of data play a decisive role in the quality of the service that can be given, whereas they are also essential on the paying side, by facilitating better targeted advertising.

A second observation relates to market power. Companies acquire market power because they accumulate large amounts of personal data and are able to diffuse those data. Article 102 TFEU does not address market power as such, but prohibits the abuse of a dominant position as being incompatible with the internal market. A breach of EU competition law could consist of an anticompetitive acquisition of data, for instance through an exclusivity agreement imposed by a search engine.\(^ {1553}\) Such a breach does not only prejudice competition as such, but also competition on privacy settings. The breach deprives consumers of the possibility to choose a search engine taking into consideration the level of privacy protection.

A specific issue in relation to market power and personal data is the concept of an essential facility,\(^ {1554}\) the idea that the owner of a facility needs to share this facility with his rivals if access to a market would otherwise be impossible or seriously impeded.\(^ {1555}\) The Court of Justice accepts that in exceptional circumstances the exercise of an exclusive right by the owner may involve abusive conduct.\(^ {1556}\) As summarised by the Court of First Instance: “the refusal of the service in question must be likely to eliminate all competition on the market on the part of the person requesting the service, such refusal must not be capable of being objectively justified, and the service must in itself be indispensable to carrying on that person’s business […]. According to settled case-law, a product or service is considered necessary or essential if there is no real or potential substitute”.\(^ {1557}\) In a market of personal

---

\(^{1550}\) These companies can be defined as “data brokers”; see: Federal Trade Commission, May 2014, Data Brokers, A Call for Transparency and Accountability.

\(^{1551}\) As explained above, in this same section.

\(^{1552}\) See on this: Damien Geradin & Monika Kuschewsky, Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, Discussion Papers Tilburg Law and Economics Center, DP 2013-010.

\(^{1553}\) Geradin and Kuschewsky allege that Google has entered into exclusivity agreements with some of the main publishers’ websites (such as Amazon.com and AOL.com) excluding other search engines from being accessible on those websites; see: Damien Geradin & Monika Kuschewsky, Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, Discussion Papers Tilburg Law and Economics Center, DP 2013-010.

\(^{1554}\) Damien Geradin & Monika Kuschewsky, Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, Discussion Papers Tilburg Law and Economics Center, DP 2013-010, at 3; European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", at 41.


\(^{1556}\) E.g., Case C-7/97, Bronner, EU:C:1998:569, at 43-46.

data, this concept of an essential facility could possibly be of use, for instance in respect of the Google search engine with a market share of more than 90%, but the threshold is high.

The previous considerations are based on the notion that personal data have become an asset and, therefore, relevant in a competition context. This would be a natural way of creating synergy between these areas of law. This synergy between competition law and privacy and data protection should be addressed by the EU legislator in further changes of the EU legislative framework, be it the rules on data protection or on competition. An approach based on synergies would also enhance the Union’s legitimacy, demonstrating that different parts of bureaucracy are capable of joining efforts in addressing challenges of the information society.

A topical subject that should be part of a possible action of the EU legislator is including considerations of privacy and data protection as such in EU competition law and enforcement. Given the fact that protection of consumers is one of the objectives of competition law,\textsuperscript{1558} this would not be illogical.\textsuperscript{1559} However, the case law of the Court of Justice of the European Union does not give a clear basis for including considerations of data protection in competition enforcement. As Advocate General Geelhoed states: “Any problems concerning the sensitivity of personal data can be resolved by other instruments, such as data protection legislation”.\textsuperscript{1560} Finally, a way of increasing synergy between competition law and privacy and data protection would be the enforcement cooperation with the authorities which are active in the two different areas.\textsuperscript{1561}

12. Privacy Rules in the US: An Introduction to the Importance of Multi-Stakeholder Solutions

The proposed General Data Protection Regulation is largely motivated by arguments on efficiency and effectiveness. Those are also the arguments the European Commission uses to motivate its proposal. The Explanatory Memorandum underlines that the “current framework remains sound as far as its objectives and principles are concerned”. A new framework is needed for other reasons. It must be stronger than the present one, more coherent and backed by strong enforcement, just to mention a few catchwords in the Explanatory Memorandum.\textsuperscript{1562}

One of the focuses in the reform is the engagement of the private sector, through multi-stakeholder solutions, empowering data controllers and making them more responsible. This

\textsuperscript{1558} As mentioned previously in this section.
\textsuperscript{1559} In the same sense, Dissenting Statement of Commissioner Harbour In the Matter of Google/DoubleClick, available on: ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.
\textsuperscript{1560} Opinion of AG Geelhoed in Case C-238/05, Asnef-Equifax, EU:C:2006:440, at 56, included in the CJEU’s ruling.
\textsuperscript{1561} Encouraging cooperation with agencies in other fields is one of the conclusions of Chapter 7 of this study.
\textsuperscript{1562} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final, Explanatory Memorandum, at “Context of the proposal”.

269
focus justifies a short look at the United States, where multi-stakeholder solutions are at the core of privacy governance.

**General features of privacy legislation in the US**

There is no general US law on privacy and data protection. The absence of a general legal framework in this area has been generally recognised as a shortcoming in the US system. Instead a number of state laws and sectoral laws exist, often described as a legislative patchwork.  

At the beginning of 2012, President Obama announced a Consumer Privacy Bill of Rights, containing a set of data privacy principles that were to be codified in legislation to be adopted by Congress. This bill of rights was to apply to the entire private sector, but not to the public sector. However, further initiatives towards such a codified set of principles in federal legislation have not been approved, most likely for reasons not related to the areas of privacy and data protection.

**US privacy legislation has a limited scope**

The most general existing law is the US Privacy Act of 1974, which gives protection to individuals against data processing by the federal government in federal records and gives them access to records relating to them. This law was adopted against the background not only of technological developments, but also of the Watergate Scandal.

The US Privacy Act has a limited scope. It does neither apply to the private sector, nor to the administration of the States. Moreover, wide exceptions are provided for, for instance in relation to intelligence and law enforcement agencies. In these domains specific regimes for protection may exist, such as the – much criticised and now to a certain extent strengthened – regime under the US Foreign Intelligence Surveillance Act.

---

1564 White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012.
1565 In the absence of legislation, this Bill of Rights should, in a first phase, be elaborated into enforceable codes of conduct. The term Bill of Rights thus does not by itself imply a legislative instrument and is not comparable to the US Bill of Rights mentioned before, which is part of the Constitution.
1566 This reason is the well-known deadlock in Congress (see, e.g.: http://www.nytimes.com/2014/07/02/us/politics/deadlock-in-congress-appears-to-worsen-as-midterms-loom.html). This was confirmed in various contacts of the author with US experts.
1569 The US Privacy Act concurs in this respect with the first laws on data protection in Europe.
One limitation to the scope that by definition affects European citizens, is that the protection under the US Privacy act does not extend to persons who are not “a citizen of the United States or an alien lawfully admitted for permanent residence”.

This limitation to the scope of protection ratione personae is in line with the case law of the US Supreme Court, for instance in United States v Verdugo-Urquidez, a case concerning the physical search of premises abroad of an alien individual without any links to the United States invoking his right under the Fourth Amendment. The protection given under the Fourth Amendment does not govern the extraterritorial search of the property of an alien who lacks sufficient connection with the United States. The draft Judicial Redress Act of 2015, currently pending in Congress, aims to mitigate the 1974 Privacy Act’s non-applicability to non-US citizens.

In addition to the US Privacy Act, privacy is protected under a range of sectoral federal laws, which – generally speaking – focus almost exclusively on companies that hold sensitive data. Examples are the Fair Credit Reporting Act (FCRA), which was originally enacted in 1970, and the 1996 Health Insurance Portability and Accountability Act (HIPAA). These laws are not confined to privacy, but ensure privacy protection in two sensitive areas. The FRCA protects against unfair and non-accurate practices of companies that collect information from various sources and provide consumer credit information on individual consumers for a variety of uses. The HIPAA regulates the use

---

1572 Section 5 U.S.C. § 552a, (a)(2).
1575 The Fourth Amendment reads: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
1582 These companies are called Consumer Rating Agencies, not to be confused with the Credit Rating Agencies that played a role in the aftermath of the financial crisis, e.g. by rating the creditworthiness of EU Member States.
and disclosure of Protected Health Information. Finally, the Children’s Online Privacy Protection Act of 1998 (COPPA) offers quite strong protection against the online collection of personal information from children under 13 years of age.

The legislative framework is completed by a large number of State privacy laws. Although discussing these laws would exceed the scope of this study, one exception can be made: the data breach notification statutes of the States requiring companies to disclose the existence of a data breach to affected customers. This is a new data protection instrument, which is widespread in the United States and has also influenced the law-making in the EU.

Non-legislative instruments in the US, a key element in consumer privacy

As illustrated by the 2012 White House Paper on consumer data privacy in a networked world, codes of conduct and other voluntary commitments by private actors are an integral part of the protection that should be given, at least in the commercial sector. The paper calls for “a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models” and, therefore, announces what is called ‘multi-stakeholder processes’ that must develop enforceable codes of conduct.

This preference for private sector leadership, including self-regulation, as the preferred approach to privacy protection is deeply rooted in the internet approach of the US government. This preference is based on the belief that privacy legislation could hamper market development in the information society. However, this preference is not unconditional: should the private sector fail to ensure protection, legislation may follow.

The important role for self-regulatory mechanisms is also linked to the fact that a large part of data protection in the private sector is considered to be general consumer protection law and, therefore, outside the scope of the constitutionally protected right to privacy. Furthermore, self-regulatory mechanisms have also been used as a vehicle to allow data transfers from the

---

1583 The HIPAA has a wider scope, also relating to health insurance.
1587 White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012, e.g., in the foreword.
1589 Obviously, as Rubinstein explains (document referred to in previous footnote), this approach led to criticism, also in the US.
1590 This was in any event an essential part of the approach by the Clinton administration (see the report quoted in previous footnote). President Obama takes it a step further by asking for legislation (until now, without success, as mentioned before).
EU under the safe harbour decision, by creating a voluntary mechanism enabling US organisations to demonstrate their compliance with Directive 95/46.\textsuperscript{1591}

A final remark in this context is that, although the wide reliance on self-regulatory mechanisms in the US contrasts with the EU approach on privacy and data protection, self-regulatory mechanisms are also promoted in the EU legislative framework, for instance in Article 27 of Directive 95/46, on the drawing up of codes of conduct. These mechanisms are even an essential instrument for the transfer of personal data to third countries. An example is the transfer by way of binding corporate rules, a practice that is intended to receive legislative recognition under the General Data Protection Regulation.\textsuperscript{1592}

The Fair Information Practice Principles, substantive standards of protection comparable to the principles in the EU

The absence of a general legal framework does in itself not mean that the substantive standards for data protection are essentially different from the standards applicable in the European Union. The United States recognise the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as amended in 2013.\textsuperscript{1593} The principles of data privacy mostly used in the US (the Fair Information Practice Principles, or FIPPs)\textsuperscript{1594} are largely comparable to those laid down by the OECD and also in Council of Europe Convention 108 of 1981, as well as in the legal instruments on data protection of the European Union.

On one point, however, there is an essential difference. An important element of the European systems is that they attach more value to the limitation of data collection\textsuperscript{1595}, whereas the United States focus on the use of data. Illustrative in this context is that one of the principles included in the 2012 White House Paper is ‘respect for context’.\textsuperscript{1596} This principle means that companies must “collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.” This approach is not very precise\textsuperscript{1597} and seems less strict than the EU approach in Article 8 Charter, as it allows greater repurposing of data. This difference is particularly relevant in the context of big data.


\textsuperscript{1593} Amended on 11 July 2013 by C(2013)79.

\textsuperscript{1594} As implied before, the FIPPs are used by the US Federal Trade Commission in its privacy practice in the commercial sector, and comparable FIPPs are also used by the Department of Homeland Security (DHS); see: Memorandum 2008-001 of 29 December 2008 of the Chief Privacy Officer of DHS, memorializing the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at the Department, available on: \url{http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf}.

\textsuperscript{1595} E.g., Article 6(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, which reads: “personal data must be […] adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”

\textsuperscript{1596} Principle 3 of the Privacy Bill of Rights.

\textsuperscript{1597} Nissenbaum proposes to specify it to context as a social domain; see: Nissenbaum in: Privacy in the Modern Age, The Search for Solutions, Marc Rotenberg, Julia Horwitz, Jeramie Scott (eds), at 152-163.
13. **Effectiveness and Conditions for Good Legislation: Engaging the Private Sector**

As has been explained above, the data protection reform aims at improving the effectiveness of privacy and data protection. This objective resulted in the choice of a regulation as the centrepiece instrument of data protection. The European Commission considers that a regulation is the best legal instrument for data protection, based on reasons – more or less – related to effectiveness. As the Commission explains, a regulation “will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.”

An essential impetus for the reform is the empowerment of individuals, data controllers and data protection authorities, as is clear from the two communications of the Commission explaining the reform. The empowerment of the data controller is implemented by a stronger engagement of the private sector, for instance through strengthening the accountability of the controller.

*Introductory remarks on engaging with the private sector*

Another perspective for analysing the EU legislator’s competence under Article 16(2) TFEU is the choice of legislative arrangements, which is crucial in the complex environment of privacy and data protection on the internet. The instruments chosen should give the right incentives to data controllers to effectively ensure protection on the internet. In the words of Bamberger & Mulligan, it is not privacy in the books that counts, but privacy on the ground. This is in line with an earlier orientation of the Commission in relation to EU legislation in general, to focus on the impact of this legislation on the ground by “paying constant attention to improving the quality, effectiveness and simplicity of regulatory acts”.

The Better Regulation Guidelines (2015) the Commission uses when preparing legislation indicate that attention be given to the internet. These guidelines recommend anticipating “technological or societal developments such as the pervasiveness of internet” and emphasise

---

1599 See the references to empowerment or strengthening the control in: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM (2012) 9 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final.
that new initiatives should operate effectively offline as well as online.\textsuperscript{1602} More generally, the legislator needs alternative approaches to traditional command-and-control legislation in order to effectively intervene in global and technologically complex environments. This is widely recognised. Rubinstein refers to modern legislative theory\textsuperscript{1603} declaring that traditional forms of state regulation are inadequate for the following reasons: costly, inefficient, intrusive, disregards the unique interests of individual businesses in favour of a ‘one-size-fits-all’ approach, fails to harness industry expertise, and stifles innovation.

Various efforts have taken place in the EU context under the umbrella of ‘Smart Regulation’.\textsuperscript{1604} Craig & de Búrca describe these developments as a shift away from hierarchical governance.\textsuperscript{1605} Shapiro mentions the downplay of command-and-control regulation in favour of negotiated, consensual regulation with the market having a role in the process.\textsuperscript{1606}

This development of shifting away from hierarchical governance is driven by the requirement of effectiveness as a condition for good legislation. However, legislation must also be based on democratic legitimacy and accountability, as was explained in Chapter 4. Democratic legitimacy is a requirement for all government intervention, but is crucial in the area of fundamental rights where essential values are at stake.

Most importantly, in the area of fundamental rights the primary responsibility remains with the government, which means, in the present context, that the EU legislator acts on the basis of Article 16(2) TFEU, with full democratic accountability. This does not preclude multi-stakeholder solutions from playing a role in this area, provided that this does not diffuse responsibility among a possibly wide range of actors.\textsuperscript{1607}

Equally, judicial accountability must be ensured. Individuals should be given the necessary tools to act and defend their rights. Where the private sector is involved in core government tasks, such as law enforcement, the requirements for judicial accountability are even higher. Good enforcement is needed, under the rule of law judicial and other remedies must be easily accessible and complete, and the mechanism of protection must be transparent for individuals.

\textit{Multi-stakeholder solutions or multi-level governance}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{1602} Commission Staff Working Document, Better Regulation Guidelines, SWD(2015) 111 final, at 23.
\item \textsuperscript{1603} Shortcomings of traditional State legislation recognised by modern regulatory theory are listed by: Ira Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, NYU School of Law, Public Law Research Paper No. 10-16, at 367. See also: Robert Baldwin, Martin Cave, Martin Lodge, Understanding Regulation, Theory, Strategy, and Practice, Second Edition 2012, Oxford University Press.
\item \textsuperscript{1604} The European Commission uses this term mostly in its policies to reduce red tape, under the umbrella of ‘regulatory fitness’; see: \url{http://ec.europa.eu/smart-regulation/index_en.htm}
\item \textsuperscript{1605} Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 159 (and the sources mentioned there).
\item \textsuperscript{1606} M. Shapiro in: Paul Craig and Grainne de Búrca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 113.
\item \textsuperscript{1607} Vandenbruwaene in: Special Issue on the Constitutional Adulthood of Multi-Level Governance of the Maastricht Journal of European and Comparative Law, 2014, Vol. 21/2, at 231.
\end{enumerate}
\end{footnotesize}
Multi-stakeholder solutions\textsuperscript{1608} is a concept that plays a key role in the governance of privacy and data protection in the United States. Governments cooperate closely with private sector and citizens’ representatives, with the aim of developing self-regulatory or co-regulatory mechanisms. In the European Union the term used is multi-level governance.\textsuperscript{1609}

Multi-level governance means that government involves various actors in the public and private sector. This involvement is expected to lead to greater responsibility of these actors.\textsuperscript{1610} Multi-level governance engaging the private sector is increasingly recognised as being necessary for effective governance\textsuperscript{1611} or, in other words, as a means for complying with the principle of effectiveness. As a result, traditional functions of the nation-state are diffused.

Directive 95/46 contains some tools which give effect to the concept of multi-level governance. Article 17 of Directive 95/46 requires data controllers to implement appropriate technical and organisational measures to protect personal data\textsuperscript{1612} and is an example of the notion of accountability, as explained below. Article 27 of Directive 95/46 provides that the Member States and the Commission shall encourage the drawing up of codes of conduct and is an example of self-regulatory or co-regulatory approaches. Multi-level governance has a far more prominent role in the Proposal for a General Data Protection Regulation, which contains a chapter on the controller and processor that is based on the notion of accountability\textsuperscript{1613} and also includes provisions on codes of conduct and certification.

The notion of accountability of data controllers and processors is an important element in the discussions on effective data protection. Accountability can be defined as a result-oriented approach, whereby the addressee of the law must ensure and demonstrate compliance, but is free in choosing the means. Basically, data controllers – private actors as well as public authorities – must translate the need to ensure respect for the fundamental rights of privacy and data protection into their daily practices.

This study discusses accountability in more detail, as a multi-stakeholder solution where governments work together with private sector and citizens’ representatives. Accountability

\textsuperscript{1608} The central term in policy discussions in the United States; see: White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012.

\textsuperscript{1609} As illustrated by the Special Issue on the Constitutional Adulthood of Multi-Level Governance of the Maastricht Journal of European and Comparative Law, 2014, Vol. 21/2.


\textsuperscript{1612} Article 17(1) of Directive 95/46. Similar measures must be taken by the data processor, under Article 17(2) and (3). To be complete, also Article 26(2) relating to data transfers contains some elements of accountability.

\textsuperscript{1613} Chapter IV of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final. This chapter of the proposal is practically in its entirety an elaboration of accountability, although the Commission proposal uses the term accountability only in the Explanatory Memorandum.
is closely related to instruments of self-regulation or co-regulation, including standardisation and certification. However, it is not the same.

14. **Accountability as an Overarching Solution for delivering Privacy and Data Protection**

In this chapter the term accountability is used in relation to those private and public actors that bear responsibility for data processing, i.e. the data controllers and the data processors in the sense of EU data protection law, whereas other parts of this study deal with accountability as a notion linked to the democratic legitimacy of governmental actors of the European Union and its Member States.

Accountability is a concept connected to corporate social responsibility, which is defined by the Commission as “the responsibility of enterprises for their impacts on society.” It requires companies to have in place “a process to integrate social, environmental, ethical, human rights and consumer concerns into their business operations.” Corporate social responsibility means that companies not only respect the law, but that they voluntarily go beyond what the law requires. The process should be led by companies themselves, with public authorities in a supporting role. Corporate social responsibility also extends to the business processes of public authorities. This responsibility is specified for the domain of human rights in a document of the United Nations High Commissioner for Human Rights: “In order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances.” These policies and processes require ‘human rights due diligence’, including the assessment of actual and potential human rights impacts, as well as reporting obligations. As explained below, these elements are all relevant for the concept of accountability in the area of privacy and data protection.

---

1614 Although, surprisingly enough, this connection is generally not made in literature on accountability in data protection.
1615 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A renewed EU strategy 2011-14 for Corporate Social Responsibility, COM(2011) 681 final, at 3.1.
1616 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A renewed EU strategy 2011-14 for Corporate Social Responsibility, COM(2011) 681 final, at 3.1.
1617 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A renewed EU strategy 2011-14 for Corporate Social Responsibility, COM(2011) 681 final, at 3.4.
In the area of privacy and data protection, the concept of accountability has various dimensions.\textsuperscript{1621} It was first developed in the context of the OECD\textsuperscript{1622} and plays a prominent role in the amended OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.\textsuperscript{1623} These guidelines state that a data controller should be accountable for complying with measures that give effect to the data protection principles. This implies that the data controller or processor, \textit{inter alia}, must have in place a privacy management programme, must be prepared to demonstrate how its privacy management programme operates and must notify security breaches affecting personal data.\textsuperscript{1624}

The two central elements, which are also included in Article 22 of the proposed General Data Protection Regulation, are that a data controller must ensure compliance and also be capable of demonstrating this. Privacy programmes, as required by the OECD, internal data protection officers within an organisation, application of the Privacy by Design principle and the carrying-out of data protection impact assessments for risky data processing operations as mentioned by the European Commission\textsuperscript{1625} are all elements of the concept of accountability. The same goes for the obligation of an organisation to issue a public report on its activities in relation to privacy and data protection.\textsuperscript{1626} A report by Nymity summarises three main elements of accountability within an organisation: responsibility of the organisation itself, ownership of the entity within the organisation responsible for personal data processing and evidence based on documentation that privacy management activities are completed.\textsuperscript{1627

Applying the concept of accountability in the area of privacy and data protection has merits because it has the potential to enhance the protection’s effectiveness. This potential has to do with various factors. The first factor is that accountable organisations are encouraged to take ownership over compliance with data protection law. It confers responsibility on those actors that are best placed to deliver protection, by encouraging them to take a proactive approach and to include data protection in daily business practices. Because controllers have been

\begin{itemize}
  \item Sections 14 and 15 of the OECD guidelines.
  \item As suggested by the European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 175. The Legislative Resolution of the European Parliament amends Article 22(3) in this direction.
\end{itemize}
involved in the design of the accountability schemes and the schemes can be tailored to their specific needs, they are more likely to follow them.\footnote{Butin, M. Chicote and D. Le Métayer, Strong Accountability: Between Vague Promises, in: Reloading Data Protection, Serge Gutwirth, Ronald Leenes, Paul de Hert (eds.), Multidisciplinary Insights and Contemporary Challenges, Springer 2014, at 354.}

The second factor is related to the first and also has to do with the creation of the schemes. Various actors may be involved in designing accountability schemes, which may enhance the quality of these schemes and may also provide an incentive for wider notions of public interest to be taken into account in the schemes. In its opinion on accountability, the Article 29 Working Party\footnote{Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, at 30.} suggests that guidance be given, for instance by data protection authorities to data controllers. In other contexts it is even proposed that data protection authorities should be actively involved in designing specific accountability schemes.\footnote{E.g., the “on-demand accountability rules” as proposed by Nymity; see: Nymity, Getting to Accountability, Maximizing Your Privacy Management Program, The Nymity Approach to Getting to Accountability, available on: \url{https://www.nymity.com/~/media/NymityAura/Resources/Getting%20to%20Accountability/Nymity-Getting-to-Accountability-Paper.ashx}.}

The third factor concerns flexibility. Accountability allows organisations to better focus the protection on processing activities that are likely to involve a “high risk” to qualified interests of individuals, such as discrimination, identity theft, fraud or financial loss.\footnote{These “high risk” categories are mentioned in Centre for Information Policy Leadership, The Role of Risk Management in Data Protection, at 10, with reference to a Council document in the context of the data protection reform package.} Flexibility is even more relevant in the absence of consensus on the meaning of risk and harm for the individual.\footnote{Centre for Information Policy Leadership, The Role of Risk Management in Data Protection, at 1.}

The fourth factor has to do with the inherent cross-border nature of data processing operations. This is the most evident factor: accountability encompasses data processing operations outside the territory of the European Union, for which an operator within the Union or with a link to the Union is responsible. Effective control is more difficult where an authority within the Union has to ensure compliance with command-and-control rules.

The fifth factor has to do with transparency. Accountability schemes – especially when they are designed to demonstrate compliance with the law – may reveal a lot about what actually happens with personal data, also on the internet. These schemes provide all those having to deal with privacy and data protection on the internet with information that can be used to improve policies or other relevant actions in this domain. Accountability thus compensates for loss of control in the era of big data.\footnote{D. Butin, M. Chicote and D. Le Métayer, Strong Accountability: Between Vague Promises, in: Reloading Data Protection, Serge Gutwirth, Ronald Leenes, Paul De Hert (eds.), Multidisciplinary Insights and Contemporary Challenges, Springer 2014, at 352-353. They mention mobile and cloud computing in connection of use of control.}

The sixth factor has to do with enforcement. Since controllers have to demonstrate compliance, there is an opportunity for enforcement, enabling data protection authorities – or
data subjects and their representatives – to act on the basis of the data controllers’ reporting. If accountability schemes work properly, enforcement by data protection authorities could become a second line of enforcement, which could allow for a more efficient use of resources, because data protection authorities could be more selective in their acts.

However, the concept of accountability also raises objections, varying from the view that accountability brings nothing new, or even accentuates the imbalance between controllers and data subjects, to technical and economic arguments.\textsuperscript{1634} An obvious economic argument is based on the criticism that it will be mainly consultants, lawyers and accountants or, more generally, experts hired to write privacy programmes and reporting tools who will profit from the implementation of the concept of accountability.

Two main objections this study identifies are: the lack of legal certainty, caused by flexibility, and the blurring of responsibilities. These two objections relate to the status of data protection as a fundamental right, which requires, as has been explained in this study,\textsuperscript{1635} a high level of legitimacy. More specifically, individuals must be empowered to invoke their right before a court and to complain before a data protection authority.\textsuperscript{1636} This requires both the rules relating to rights and obligations, and the responsibilities to be unambiguously identified.

This leads to the following conclusions. Accountability is an effective and legitimate instrument for the governance of privacy and data protection, since it places emphasis on the social responsibility of companies and public authorities in carrying out their respective business and policy practices.

Accountability schemes, such as company privacy programmes, should be sufficiently precise in order to ensure that data subjects or other affected third parties are able to understand their rights and obligations. The relation of these schemes to the provisions of EU data protection law should be fully transparent.

Prior involvement of public authorities – in particular data protection authorities – may be advantageous for controllers and may promote the compatibility of accountability schemes with EU data protection law, but should not bind these authorities in the exercise of their enforcement role, in particular where they are acting in response to individual complaints. Co-responsibility of data protection authorities – for instance through endorsement of accountability schemes – is to be avoided.\textsuperscript{1637}


\textsuperscript{1635} E.g., in Chapter 4.

\textsuperscript{1636} As specified in Article 28 of Directive 95/46.

15. Conclusions

The mandate of the European Union to act under Article 16 TFEU is widely formulated, and gives the Union the opportunity to deliver upon its ambitions. Article 16(2) TFEU must be seen as an explicit choice in the Treaty to bring data protection to the Union level, by giving the European Parliament and the Council, in their common capacity as EU legislator, the duty to lay down the rules.

The material scope of the rules must include all personal data. An exception to the material scope, excluding certain types of personal data, cannot be laid down in secondary EU law. The data protection reform – with the General Data Protection Regulation as its centerpiece – should lead to the full implementation of this obligation of the EU legislator, also in domains where at present EU rules are lacking. Article 16(2) TFEU is a shared competence between the Union and its Member States, but there is not much autonomous room for the Member States to adopt legislation in this area. The entry into force of the General Data Protection Regulation, in particular, will take away most of the Member States’ autonomy.

In exercising its mandate, the EU legislator must take account of the Union’s competences in other areas, as well as the Member States’ legitimate claims for competence. EU data protection has an impact on core competences of Member States and, therefore, they have a legitimate role to play, although often by delegation. The Union acts internally within a pluralist legal context, with an important role for the Member States in accordance with the principle of subsidiarity. (Section 2)

There is one EU legislator, although it is composed of different institutions. The input of the three institutions, respecting the institutional balance, provides the mandate of the EU legislator with democratic legitimacy, with the nuances explained in Chapter 4. The positions the institutions take in data protection and their input in the negotiations on the data protection reform also reflect institutional concerns. As a rule, the European Parliament acts as a supporter of strong privacy and data protection, the Council represents national concerns and the Commission is committed to integration. Hence, the outcome of the legislative process by definition has the features of a compromise. (Section 3)

The EU legislator involves the Member States and the private sector and civil society. Involvement of these various stakeholders in the decision-making process must give the procedure further democratic legitimacy, and produce an outcome that takes into account the different interests at stake. Integration as a result of Article 16 TFEU is not a goal in itself but an instrument to enhance internet privacy and data protection, which includes the bureaucratic capacity to deliver and aspires to public acceptance of EU involvement. (Section 4)

The mandate under Article 16 TFEU presents a parallel with the competence of the EU legislator under Articles 18 and 19 TFEU on equal treatment and non-discrimination. Both mandates have their origins in the internal market, but now deal with fundamental rights. Due
to this increased status, high standards of effective protection are observed in both areas. However, under Articles 18 and 19 TFEU, the Member States may claim wider discretionary powers and require a higher level of protection under national law. These discretionary powers do not exist under Article 16 TFEU, for instance because of the importance of a uniform level of data protection in the digital single market. (Section 5)

The European Data Protection Supervisor has identified four categories of provisions where the Member States should exercise competence in privacy and data protection. These are: where EU law builds on national law to provide a ground for processing personal data, for instance in the public interest; where EU law mandates national law to give effect to its provisions, for instance where it obliges the Member States to establish data protection authorities; where EU law allows or requires national law to specify EU rules; and where EU law allows or requires national law to depart from EU rules. This study adds a fifth category: provisions enabling the Member States to balance privacy and data protection with other fundamental rights, within their field of competence. (Section 6)

The EU legislator is – in the exercise of its mandate – confronted with interfaces with other competences of the Union and the Member States in related areas. These interfaces impact the mandate under Article 16 TFEU. This study identifies specific areas where interfaces exist: the freedom of expression and information where the EU has limited competence but where internet developments can have a big impact on the enjoyment of the freedom; open data and the interface between transparency and data protection; and measures for internet monitoring with the aim of enforcing intellectual property rights. (Section 7)

Legitimacy also requires the EU legislator to address the interfaces of privacy and data protection with security in an intelligent manner, taking into account the case law of the Court of Justice. Security is a priority both for the European Union and its Member States, and national and EU laws are adopted allowing a wide use of personal data for security purposes. The EU competences in the area of freedom, security and justice focus on the coordination and cooperation between the Member States for reasons of security. The exercise of these competences – for instance through EU legislation – facilitates the exchange of large amounts of personal data between police and judicial authorities on national and EU level, but should not unduly impact on everyone’s right to privacy and data protection. (Section 8)

Important synergies exist between privacy and data protection on the one hand, and economic interests on the other hand. Addressing these synergies is primarily a task of the EU legislator and not of the Court of Justice, which adjudicates when there are disputes, but not where synergies between different areas of intervention can be found. Using synergies in different areas of intervention by the Union and the Member States enhances the legitimacy of the EU legislator’s contribution under Article 16 TFEU.

Privacy and data protection are intended to create trust, thereby positively influencing – or even boosting – growth and innovation, for instance in connection with the Digital Agenda for Europe. Privacy by Design is the prime example, given that it is aimed at enhancing trust
in data protection whilst creating economic incentives. It should thus also be an instrument in economic policies of the Union. Moreover, the right to data protection itself provides for a system of checks and balances and allows processing of personal data so long as requirements of fairness and lawfulness are satisfied. (Section 9)

The legal framework for electronic communications may create synergy, in addition to Directive 2002/58 on privacy and electronic communications, since it gives governments responsibility in network governance, in contrast with the governance of the internet infrastructure, with little role for governments. Government responsibility in network governance could be used for enhancing control over the processing of personal data. In consumer protection, Directive 2005/29 on unfair commercial practices prohibits misleading omissions and requires transparency in business-to-consumer transactions. A misleading practice directly related to internet privacy and data protection is the offering of ‘free’ services on the internet, where individuals pay with their personal data. This directive in the field of consumer protection could also be used to require from internet services to apply transparent privacy policies. The EU legislator should consider addressing these synergies. (Section 10)

Competition law is relevant in the context of this study, because of the asymmetric structure of the information economy. In this economy, personal data have become an asset, which leads to companies acquiring market dominance precisely because they accumulate large quantities of personal data. This synergy between competition law and privacy and data protection should be addressed by the EU legislator in further changes of the EU legislative framework. A topical subject that should be part of such change is including considerations of privacy and data protection as such in EU competition law and enforcement. At present, these are areas of EU intervention with little interconnection. However, an approach based on synergies would enhance the Union’s legitimacy, demonstrating that different parts of bureaucracy manage to join efforts. (Section 11)

The approach to governance in respect of privacy and data protection in the United States provides some insight in the importance of multi-stakeholder solutions, in which the private sector is engaged, as a means to provide effective protection. In the US non-legislative instruments are a key element in consumer privacy, in the absence of a general US law on privacy and data protection. Engaging the private sector is a trend in the EU as well, also in the exercise of the mandate of the EU legislator under Article 16(2) TFEU. (Section 12)

The choice of legislative arrangements is crucial in the complex environment of privacy and data protection on the internet. The European Commission recognises the need for specific arrangements that anticipate the developments on the internet, more generally, in its Better Regulation Guidelines of 2015 and in its policies under the umbrella of Smart Regulation. Effective enforcement is needed, under the rule of law judicial and other remedies must be easily accessible and complete, and the mechanism of protection must be transparent for the individual. Multi-stakeholder solutions and multi-level governance are concepts that play an increasing role in the governance of privacy and data protection in the European Union. (Section 13)
Accountability of data controllers and data processors should play an important role as a legislative technique, allocating responsibility to data controllers. Accountability, as a concept, is connected to corporate social responsibility and an alternative for command-and-control legislation, based on general notions of quality of legislation. Accountability schemes, such as company privacy programmes, should be sufficiently precise. The relation of these schemes to the provisions of EU data protection law should be fully transparent. Prior involvement of data protection authorities in accountability schemes should not bind these authorities in the exercise of their enforcement role, in particular where they act in response to individual complaints. (Section 14)

Finally, the expected adoption of the General Data Protection Regulation – an EU regulation replacing an EU directive – as main instrument for data protection is an appropriate choice of a legislative instrument. This regulation should not only ensure a high, but also a harmonised level of protection. A distinctive approach for the public sector does not appear an appropriate choice of instrument: there should be no distinction in law between the private and public sectors, the individual deserving equal protection in both sectors, in the entire European Union. The fact that the Member States play and should play an important role should not result in a non-satisfactory choice of instruments.
Chapter 7. Understanding the Role of Independent, Effective and Accountable DPAs: New Branches of Government in between the Union and the Member States

1. Introduction

The independent data protection authorities (“DPAs”) are a further group of actors that shape the landscape of data protection within the European Union. Their task is to enforce the laws, or in the terms of primary EU law: to ensure independent control on the rules on data protection. The Court of Justice of the European Union regards these authorities as the guardians of data protection.\(^{1638}\)

This chapter analyses the contribution of the DPAs under Article 16 TFEU, an element of the research question on the role of the European Union, which is specified as: “what does and should the European Union do to make Article 16 TFEU work, through control by independent authorities?” This analysis includes the following subjects:

- a. the general design of the contribution by DPAs derived from primary law and recognised as being essential in an information society;
- b. reasons of existence, a variety of roles and a different system in the United States;
- c. DPAs as a new branch of government, different but similar to EU agencies, and a theory on expert bodies; the hybrid position in between the European Union and the Member States;
- d. complete independence of DPAs as specified in the case law of the Court of Justice;
- e. a presumed lack of effectiveness of DPAs;
- f. democratic and judicial accountability of DPAs;
- g. conclusions with a model for good governance by DPAs.

In other words, this chapter analyses the legitimate role of the DPAs in ensuring the control over the fundamental rights of privacy and data protection on the internet. It focuses on the constitutional position of the DPAs and on their tasks.

The first objective of the chapter is to position the DPAs as new branches of government in between the Union and the Member States. The second objective of the chapter is to set the conditions for reconciling the requirements of independence, effectiveness and accountability. DPAs are independent, they must effectively exercise their tasks, but they act within the constitutional frameworks of the Union and the Member States and cannot escape accountability.

\(^{1638}\) Case C-518/07, Commission v Germany, EU:C:2010:125, at 23.
In the area of data protection, independent control is an essential component of the protection of the individual. The DPAs have a responsibility in supervising compliance that does not exist in most other areas of law, in any event not in the field of the protection of other fundamental rights. There is a similarity with autonomous agencies operating in a number of other areas, for instance where these bodies are set up to ensure supervision of the markets. The DPAs as well as these agencies are expert bodies exercising public tasks at a certain distance from the traditional governmental structures that are characterised by the separation of powers under the traditional _trias politica_ or – in case of the European Union – the institutional balance.

However, there are also significant differences, because of the DPAs’ specific tasks – fundamental rights, not market supervision – and because of the fact that the DPAs do not exercise their tasks on the basis of powers delegated to them by governmental bodies. Their independent role results directly from the Treaties.

Section 2 sketches the general design of the DPAs: expert bodies with constitutional status and with importance in the information society. The embedding of the DPAs in primary law gives the DPAs constitutional status. Sections 3 and 4 of this chapter discuss the reasons behind the existence of the DPAs and the competences of these authorities, that have a variety of tasks, including more policy oriented roles. Section 5 succinctly describes the different model in US law that does not work with DPAs but grants a strong role to the Federal Trade Commission in respect of consumer privacy.

Sections 6-8 introduce the notion of non-elected or non-majoritarian expert bodies, which are a model for DPAs. Section 6 explains the example of electronic communications, showing the difference between regulatory authorities in most areas of EU law and DPAs. However, they are also similar. Section 7 develops a theory on expert bodies – the rise of the unelected, as explained by Vibert for DPAs. This notion is particularly relevant because the DPAs operate in between the European Union and the Member States (Section 8).

Sections 9 and 10 analyse the requirements of independence under the Court of Justice’s case law, confirming the DPAs’ status as new branch of government. Sections 11 and 12 discuss the effectiveness of DPAs, focusing on their presumed lack of effectiveness and their struggle for resources. Most importantly, effectiveness must be ensured in the information society. Sections 13 and 14 explain the accountability of the DPAs. Independence does not preclude the DPAs from being accountable to the judiciary and free from parliamentary influence. In contrast, DPAs as expert bodies should act in a controllable and non-arbitrary manner.

---

1639 Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, as confirmed, most recently, in Case C-362/14, Schrems, EU:C:2015:650, at 42. See also the preamble to Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, stating “Convinced that supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data”.

Section 15 contains this chapter’s conclusions. Although the findings of this chapter relate to privacy and data protection they are also relevant for autonomous or independent control in other domains. The model of independent authorities may be attractive for other domains characterised by large asymmetries in knowledge and power.

### 2. The General Design of the DPAs: Expert Bodies with Constitutional Status and with Importance in the Information Society

Article 16(2) TFEU, second sentence, reads: “Compliance with these rules shall be subject to the control of independent authorities.” These rules are the rules relating to data protection and free movement of data. This provision is closely linked to Article 8(3) Charter that is worded slightly differently: “Compliance with these rules shall be subject to the control of an independent authority.”

An essential part of the enforcement of EU data protection law is assigned to expert bodies, which are primarily the DPAs of the Member States. These DPAs are independent public authorities that fulfil an important public task, but they are not accountable for their performance to the democratically elected bodies. The requirements for independence are high, according to the case law of the Court of Justice of the European Union.\textsuperscript{1641} The high requirements for independence of DPAs also result from the scope of their role, which not only includes the supervision of market actors but also the supervision of the EU institutions and national governments themselves.

This chapter analyses how the independence and effectiveness of the DPAs can be best reconciled with requirements of accountability, in a democratic society under the rule of law. In other words, how to deal with what Scholten, in the context of EU agencies, calls the classic accountability-independence dilemma.\textsuperscript{1642} Another element of the analysis is that the role of guardian of EU data protection law is attributed by primary EU law to national authorities. As national authorities DPAs are responsible for the application and enforcement of EU law within the Member States. Their position is to a certain extent hybrid, as they are attached both to the constitutional frameworks of the Member States as well as to that of the European Union. This analysis has implications for the positioning of the DPAs, as well as for the tasks attributed to them and the exercise of these tasks.

*The embedding of the role of DPAs in primary law gives them constitutional status*

Article 16(2) TFEU and Article 8(3) Charter\textsuperscript{1643} confirm the role the DPAs already have in the EU instruments on data protection, in particular Directive 95/46, which formed a basis for

---


\textsuperscript{1643} To be complete, DPAs are also referred to in Article 39 TEU. This provision will not be discussed separately in this study, for the reasons mentioned in Chapter 4, Section 2, and Chapter 6, Section 2.
Although the Lisbon Treaty codifies an already existing framework for control, the fact that this control is now embedded in primary law has substantive effects and gives the DPAs constitutional status.

The control by these authorities is not only an essential part of enforcement, it is even qualified as “an essential component of the protection”\(^\text{1645}\) itself. In other words, EU law does not only provide for institutions with a specific responsibility for the protection, but it gives the right to data protection an institutional dimension.

DPAs as independent public authorities for data protection are a unique phenomenon in EU law. This specific position is, in the first place, the result of the constitutional foundation of the role of the DPAs in primary law. The Court of Justice emphasises the autonomous nature of the interpretation of Article 28(1) of Directive 95/46 on data protection,\(^\text{1646}\) a provision that since the entry into force of the Lisbon Treaty is derived from primary EU law.\(^\text{1647}\) Primary law – the TFEU as well as the Charter – attributes the task of supervising compliance with data protection rules directly to the DPAs, whereas in most other areas of EU law the institutions delegate parts of their tasks under the Treaties to bodies of experts, such as EU agencies. The fact that the role of the DPAs is attributed under primary law and not delegated by institutions means that the DPAs cannot be considered as ‘agents’ exercising certain tasks of ‘principals’, a metaphor that plays an important role in the literature on EU agencies.\(^\text{1648}\)

The Treaties have positioned the DPAs as independent bodies with a constitutional nature responsible for a specific aspect of EU law, namely the control on the rules on data protection. The DPAs have to fulfil their tasks within the constitutional frameworks of the Member States, based on a separation of powers or trias politica, but they are not part of it, and within the constitutional framework of the Union, which is characterised by a closed system of institutional balance\(^\text{1649}\) of powers as intended by the Treaties,\(^\text{1650}\) but they are equally not part of it. Possibly, with a wide interpretation of Article 298 TFEU as explained in the ReNEUAL project, the national DPAs can be regarded as part of the European Administration. They are definitely not EU bodies.\(^\text{1651}\)

Information society

---

1645 See footnote 1639.
1646 Case C-614/10, Commission v Austria, EU:C:2012:631, at 40.
1647 Case C-614/10, Commission v Austria, EU:C:2012:631, at 36; Case C-288/12, Commission v Hungary, EU:C:2014:237, at 47.
1649 Case 9/56, Meroni, EU:C:1958:7, at 152.
1651 Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure: Introduction to the ReNEUAL Model Rules, pp 14–18. The EU Administration will be explained in Chapter 8, Section 8.
The positioning of DPAs is unique within the framework of the Treaties and already for this reason an interesting object of study. However, it is even more interesting to analyse their role in the light of the loss of control over information in the internet society as a result of phenomena like big data and mass surveillance, which reflect large asymmetries in knowledge and power. The DPAs are an additional tool for oversight on the use of information and are an additional instrument to regain trust in governments and in the European Union, provided that the DPAs operate in an independent, effective and accountable way. In the information society, their role is justified by the size of the issues at stake, based on the hypothesis that traditional methods are not sufficient.

An additional factor is that, in the information society, the control of data protection has an inherent cross-border nature. The control the DPAs have to ensure is, as a rule, confined to their national territories, but this also includes the examination of cases with a cross-border nature, for instance in the basis of a complaint vis-à-vis a data controller in another Member State.

International cooperation belongs to the core of their activities. Chapter 8 will address the specific complexities relating to this cross-border nature. DPAs are public authorities of the Member States and part of the national administration with as their primary task safeguarding privacy and data protection of individuals within their national jurisdictions. However, the DPAs are attached to the constitutional framework of the European Union, and in that role they cooperate with their peers in other Member States and with European bodies and structures. The DPAs exercise their task of ensuring control to a certain extent also outside the national jurisdiction where they are established, otherwise they would not effectively ensure that the rights of individuals are respected. This is particularly necessary in an internet environment.

3. The Institutional Background: Six Reasons for the Existence of DPAs

The history of DPAs in the EU

The independent supervisory authorities were first introduced in the EU legal framework, with Directive 95/46 on data protection, but they previously existed in a number of Member States. A well known example is the French DPA, the Commission Nationale de l’Informatique et des Libertés (CNIL), that started its activities in 1978. Other authorities

---

1652 In particular Chapter 3 of this study.
1653 As is, e.g., claimed in relation to judicial oversight by Jack M. Balkin, “The Constitution in the National Surveillance State”, Minnesota Law Review 93/1, at 22.
1655 Case C-230/14, Weltimmo, EU:C:2015:639, at 54.
1656 The demarcation between these two chapters of this study largely follows the distinction between Chapters VI and VII of the Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
were established in the 1970s, for instance in Sweden and in some German Länder. Under Article 28 of Directive 95/46 each Member State must establish one or more public authorities responsible for data protection. At present Germany and Spain use the possibility of having more than one DPA: they have a national DPA, as well as regional DPAs. The same situation exists in Switzerland, though not a Member State of the European Union.

Article 286 of the EC Treaty, introduced by the Treaty of Amsterdam in 1997, guaranteed supervision on data processing by EU institutions and bodies, for the first time mentioning supervision of data protection at the level of primary EU law. Article 286 EC was the legal basis for the foundation of the European Data Protection Supervisor (EDPS), the DPA responsible for data protection within EU institutions and bodies.

In the European Union, the national DPAs have also enjoyed constitutional status since the entry into force of the Lisbon Treaty in 2009. This constitutional status further determines their position.

**Six reasons behind their existence**

The reasons behind the existence of independent DPAs have not yet been properly analysed in comprehensive academic literature. Particularly, little has been said why, in comparison, in other areas of law the DPA model is not chosen, or why other approaches under civil, administrative or criminal law were not considered to be satisfactory for data protection.

Even more surprisingly, these reasons do not play a decisive role in the ongoing reform of the EU data protection legislation. The Commission simply states that the role of the Data Protection Authorities (DPAs) is essential for the enforcement of the rules on data protection, and that therefore their status and powers should be strengthened, clarified and harmonised.

We mention six reasons for the existence of DPAs under EU law.

First, historical reasons leading to a harmonisation of existing practices are a justification for including DPAs in instruments of EU law. Hustinx recalls the social and political preferences in the 70s of the last century to have a public authority dealing with data protection.

---

1658 G. González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series 16, 2014, Chapter 3.
1659 Under Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8/1.
1660 Some indications why these other approaches would have been less appropriate were given by P. Hustinx in Reinventing data protection?, S. Gutwirth, et al. (eds), Springer 2009, at 131.
1661 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010), 609 final, at 17-18.
1662 In an article on the EDPS (2006) I gave five reasons for the establishment of the EDPS: the need for harmonisation, the need for effective data protection as fundamental right, the fact that this fundamental right is not protected by itself, the principle of good governance and fact that existing bodies cannot sufficiently fulfil the necessary tasks, H. Hijmans, The European data protection supervisor: The institutions of the EC controlled by an independent authority, CMLR 43 (2006), at 1323-1324. These five reasons are all valid in connection to DPAs in general, but there is more to say to it.
1663 P. Hustinx in Reinventing data protection?, S. Gutwirth, et al. (eds), Springer 2009, at 131-137.
Simitis notes that neither intervention by the data subject nor any other traditional control mechanism was seen as offering sufficient guarantees. However, there were wide differences in responsibilities. Directive 95/46 on data protection harmonises these differences to a certain extent. Harmonisation is also how the Council of Europe explains its Additional Protocol on supervisory authorities adopted in 2001. According to the Explanatory Report to this Protocol, most countries with data protection laws have supervisory authorities that “provide for an appropriate remedy if they have effective powers and enjoy genuine independence in the fulfilment of their duties”. This instrument of the Council of Europe fosters harmonisation and cooperation.

Second, their existence is justified by the need for effective protection of citizens’ rights and for enforcement of the law. The right to data protection requires structural support. As Bennett & Raab observe: “laws are not self-implementing and the culture of privacy cannot securely establish itself without an authoritative champion”.

Third, the nature of data processing and the skills required to understand data processing are identified as reasons for the existence of DPAs. The secrecy or invisibility as an element of data processing requires an organisation that has the powers to protect the individual in a proactive manner. Moreover, dealing with data protection requires technical expertise. Simitis explains that the technical knowledge needed for effective supervision must be combined with the necessary intensity of this supervision.

Fourth, there is the need for control of the private sector, but equally of governments themselves, where they process personal data. This requires, on the one hand, a consistent approach to these different sectors – at least this is the choice underlying EU data protection law – and, on the other hand, an effective mechanism to supervise governments, operating at some distance from the traditional branches of government.

---

1666 Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, at 4.
1667 Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, at 9 and 10.
1671 E.g., Directive 95/46 equally applies to the public and private sector and the ‘comprehensive approach’ was a cornerstone for the Commission in the reform of the EU data protection laws, as is illustrated by Communication from the Commission to the European Parliament, the Council, the European Economic and
Fifth, as underlined by the Court of Justice of the European Union in its case law on the independent data protection authorities\textsuperscript{1672} there is a need for independence from political preferences. This is an essential difference with autonomous agencies.\textsuperscript{1673}

Sixth, there are the advantages of an organisation dedicated solely to privacy and data protection. Such an organisation can combine expertise with flexibility, for instance when deciding to investigate a presumed breach of data protection law, or where cooperation with other authorities is needed. Such other authorities can be authorities within the same jurisdiction in related areas of law, or authorities in other jurisdictions, within and outside the European Union. Moreover, DPAs have the advantage that they can dedicate their resources fully to data protection, and do not need to weigh the use of resources with other policy objectives in their area of responsibility. This argument relates to the use of resources and must not be confused with the need for weighing other policy objectives, where DPAs take decisions on data protection.

4. The Competences of DPAs: A Variety of Roles

Article 16(2) TFEU and Article 8(3) Charter lay down the task of the DPAs to ensure compliance with the data protection rules. These provisions and their implementation in EU law and national law must ensure the ‘legality’\textsuperscript{1674} or ‘role clarity’\textsuperscript{1675} of the DPAs.

These provisions of primary law give a mandate to the DPAs. Article 8(3) Charter and Article 16(2) TFEU reflect that the system of control is a complete system: Compliance shall be subject to control of these independent authorities, operating with a high degree of independence as confirmed in the case law of the Court of Justice of the European Union. This does not mean that others – like for instance national ombudsmen or agencies in neighbouring areas – cannot be competent, but their competence cannot derogate from the competence of the DPA.

At the same time Article 8(3) Charter and Article 16(2) TFEU limit this task. This section analyses three limitations: the limitation to privacy and data protection, the limitation relating to ensuring control of compliance and the limitation relating to the role of the DPAs as offering a remedy for individuals against breaches of EU data protection law.

The first limitation: Article 16(2) TFEU and Article 8(3) Charter are imprecise, but privacy and data protection are meant in a wide sense
In relation to the EDPS, the Court of Justice has declared that the competences of this DPA are circumscribed within the limits deriving from the task entrusted to them.\textsuperscript{1676} We use this formula for the circumscription of DPAs in general.

Article 16 (2) TFEU and Article 8(3) Charter entrust the DPAs with a number of tasks, albeit in an imprecise manner. The Charter was enshrined in the Treaty of Nice (2000) as a non-binding document\textsuperscript{1677} and predates the TFEU. It refers to DPAs as responsible for ensuring the control of “these rules”, whereas neither Article 8(1) nor Article 8(2) Charter mention rules.

At first sight it appears that this reference relates to the rules under Article 16(2) TFEU, first sentence. As a result Article 16(2) TFEU and Article 8(3) Charter imply a limitation that may be understood in a way that only the rules relating to the protection of personal data are covered, meaning that the rules on the use of personal data are not subject to the control of the DPAs. We argue that such a narrow interpretation would not do justice to the principle of effectiveness, nor be in line with the interpretation that the control by a DPA is “an essential component of the protection”\textsuperscript{1678} itself. This means that the control by a DPA is required wherever the right to data protection is affected, which is the case where a legal instrument enables the use of personal data.

However, this does not specify the competences of a DPA either. Privacy and data protection have interfaces with other fundamental rights and public interests.\textsuperscript{1679} The DPAs have a role to play in relation to these interfaces – to ensure privacy and data protection –, but it is not clear to what extent they are competent. For instance, do they have any competence in relation to a request for access to documents containing personal data?

The second limitation: ensuring control of compliance is not limited to enforcement strictu sensu

One could interpret “ensuring control of compliance” as meaning that Article 16(2) TFEU and Article 8(2) Charter only cover enforcement of data protection law and do not cover other tasks allotted to DPAs, such as advisory tasks. One could also interpret these provisions more broadly as covering these other tasks based on the reasoning that these other tasks are intended to ensure the practical effect of the provisions of primary law.\textsuperscript{1680}


\textsuperscript{1678} Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, as confirmed in Case C-518/07, Commission v Germany, EU:C:2010:125, at 23.

\textsuperscript{1679} As has been explained in this study, mainly in Chapters 5 and 6.

\textsuperscript{1680} This argument was used by the Court of Justice in admitting the EDPS to intervene before it. The power to intervene was “intended to ensure the practical effect” of (the former) Article 286 EC Treaty, Order of the Court of 17 March 2005, EU:C:2005:189 in Joined cases C-317/04 and C-318/04, European Parliament v Council Union (C-317/04) and Commission (C-318/04), EU:C:2006:346, at 15.
This latter interpretation confirms the choice to confer a wide variety of tasks to the DPAs. Primary EU law indicates that certain tasks must be given to DPAs. Article 28(3) and (4) of Directive 95/46 contain enforcement powers, namely powers of investigation, powers of intervention, powers to hear claims, as well as powers to engage in legal proceedings.\footnote{1681} Since Directive 95/46 is one of the bases of Article 8 Charter\footnote{1682} we argue that primary law requires these tasks to be given to the DPAs. Moreover, since these tasks are now grounded on primary law, the EU legislator can no longer withdraw these tasks.

Article 28 of Directive 95/46 also mentions other tasks that are not enforcement \textit{strictu sensu}. Under Article 28(2) of Directive 95/46 the DPAs must be consulted when governments are drawing up administrative measures or regulations. Furthermore, an obligation is laid down to draw up regular reports on activities and to cooperate with other DPAs. These tasks derive from Directive 95/46 but do not directly ensure compliance. One could qualify these tasks as supporting, intended to ensure the practical effect of compliance.\footnote{1683} Based on this qualification we argue that the EU legislator retains discretionary power in respect of these supporting tasks, provided that the result – compliance with practical effect – is achieved.

\textbf{The third limitation: the remedy before a DPA is not exclusive}

The remedy before a DPA is part of a system of remedies that is multi-layered.\footnote{1684} Article 8(2) Charter gives the individual a right to access his personal data, to be exercised against the data controller, and under Article 47 Charter everyone has the right to an effective remedy before a tribunal, against violations of EU law.

The administrative remedies before the DPA are not exclusive, but constitute a layer situated between the remedies that are available before the data controller and before a court.\footnote{1685} This is well illustrated by Directive 95/46. Article 12 of this directive gives the data subject the right to obtain from the controller specific information about the personal data about him or her that this controller is processing. This right to access also includes a right to the rectification, erasure or blocking of personal data, in particular because of the incomplete or inaccurate nature of the data.\footnote{1686} The data subject can exercise his right to access against the data controller, but can also directly involve a DPA.
Moreover, Chapter III of Directive 95/46 contains specific judicial remedies, in addition to the administrative remedies before a DPA. A data subject has a judicial remedy against any breach of data protection law and is entitled to compensation for damages. In other words, the data subject has a right to directly invoke his right before a court, as an alternative for involving a DPA. This alternative plays a role in the pending case Rease and Wullems.\textsuperscript{1687} The referring national court – the Council of State of the Netherlands – asks whether a DPA would be allowed to set priorities, which result in abstaining from enforcement upon a complaint by an individual. Possibly, the DPA has this discretion because of the existence of an alternative remedy.

\textit{Further tasks of DPAs: the attribution of powers must be sufficient to ensure control}

Further tasks of DPAs may be required under secondary EU law or under national law. These tasks of the DPAs do not only extend to enforcement \textit{strictu sensu}, but are of a more general nature, such as advising legislators and administrators and raising the awareness of the public on data protection related issues. To a certain extent the DPAs also exercise rule-making powers. The guidance provided by the DPAs and by the Article 29 Working Party\textsuperscript{1688} could qualify as a soft way of rule-making. The Fundamental Rights Agency reports that there is a wide variety in the duties and powers that the Member States have handed to the DPAs.\textsuperscript{1689} At the EU level, a wide scope of duties and powers is listed in Regulation 45/2001\textsuperscript{1690} in relation to the EDPS.\textsuperscript{1691} This was the inspiration for the lists included in the proposed General Data Protection Regulation.\textsuperscript{1692}

Although most tasks are not based on primary law, the attribution of powers must be sufficient to ensure control, as required by Article 16(2) TFEU and Article 8(3) Charter. This also requires judicial remedies, liability and sanctions, as currently foreseen in Chapter III of Directive 95/46. The Member States have implemented this chapter in a manner demonstrating that big differences between them still exist and which is not fully satisfactory.\textsuperscript{1693} The Commission Proposal for a General Data Protection Regulation includes a detailed provision for administrative sanctions, providing for financial sanctions that are much higher than those currently available in the Member States.

Finally, the discretionary powers of the national legislator are expected to significantly diminish after the entry into force of the General Data Protection Regulation.

\textsuperscript{1687} Case C-192/15, Rease and Wullems (pending).
\textsuperscript{1688} For instance, in its opinions on general concepts on data protection law, referred to at various places in this study.
\textsuperscript{1689} Fundamental Rights Agency, Data Protection in the European Union, the role of National Data Protection Authorities, 2010, mainly Chapter 4.
\textsuperscript{1690} Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8/1, Articles 46-47.
\textsuperscript{1691} As explained by H. Hijmans, The European data protection supervisor: The institutions of the EC controlled by an independent authority, CMLR 43 (2006), at 1323-1324.
\textsuperscript{1692} Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final, Articles 52-53.
\textsuperscript{1693} Fundamental Rights Agency, Data Protection in the European Union, the role of National Data Protection Authorities, 2010, at 4.3.
A variety of roles raising questions

In short, DPAs have a variety of roles. Bennett & Raab distinguish the roles of ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers. In a paper on the European Data Protection Supervisor we also mentioned this DPA as having the functions of a handler of complaints, a center of expertise, a function of ensuring the correct application of the law, offering legal protection, a regulator and finally a “constitutional function”. These roles are not very different from the roles given to EU agencies and national agencies, varying from policy oriented tasks (like advising on new legislation) to quasi-judicial functions where decisions must be taken vis-à-vis individuals.

The roles may sometimes conflict with each other. For example, in its role as a policy advisor, the DPA may oppose the compatibility of a proposed legal instrument with principles of data protection. However, after adoption of the instrument, the DPA has to enforce the instrument, in its role as an enforcer.

Another conflict may arise where DPAs cooperate with private entities, in developing frameworks for compliance of privacy and data protection, whereas they may be called upon to independently assess these frameworks in a later stage in the context of a complaint procedure. This is what Ottow describes as a horizontal style of supervision, focusing on cooperation with the supervisee. There is a risk that engaging in a dialogue with the private sector may complicate enforcement in the event of a later – alleged – breach of data protection law. This is in particular the case where DPAs engage with private parties in the implementation of more general legislative arrangements such as accountability as provided for in Article 22 of the General Data Protection Regulation.

This engagement may vary from developing general frameworks for accountability to specific consultations between individual data controllers and DPAs. In the latter situation

1697 Jóri describes this role as shaping data protection law, taking the perspective of a privacy advocate, András Jóri, Shaping vs applying data protection law: two core functions of data protection authorities, International Data Privacy Law, 2015, Vol. 5, No. 2.
1699 As Chiti formulates, in relation to EU agencies, it may make the authorities “excessively permeable” to private parties. E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), at 1395-1442, at 1401.
1700 See Chapter 6, Section 14 of this study.
1701 Examples on https://www.informationpolicycentre.com/accountability-based_privacy_governance/.
the DPAs may actively contribute to the solution, and hence be limited in their discretion at the stage of enforcement, even upon a complaint by an individual. Engagement processes must address potential conflicts of interests of participants and guard against the risks that the regulator may (be seen to) be captured by special interests.\textsuperscript{1703}

These are just examples of how different tasks may possibly compromise the core task of DPAs under primary EU law, which is ensuring compliance with EU data protection law. However, in general, it is the combination of roles that established the DPAs as strong actors in ensuring privacy and data protection. This is what makes the DPAs, in Bennett & Raab’s words “authoritative champions”.\textsuperscript{1704}

As required by EU law, the DPAs necessarily have decision-making powers. However, this does not comprise rule-making powers, which contrasts with the situation in the United States where rule-making powers are at the core of the tasks of the Federal Trade Commission.\textsuperscript{1705} Rule-making powers of expert bodies have traditionally been looked at in a critical manner within the context of EU law. This critical approach has even resulted in a renaming of what the Commission used to call regulatory agencies\textsuperscript{1706} into decentralised agencies.\textsuperscript{1707}

The case law of the Court of Justice however became, in recent years, more open towards giving rule-making powers to expert bodies. Before, in the light of Romano,\textsuperscript{1708} EU law presumably prohibited conferring legislative powers on bodies other than the EU legislature.\textsuperscript{1709} In United Kingdom of Great Britain and Northern Ireland v European Parliament and Council (ESMA)\textsuperscript{1710} the Court changed its position, based on the amendment of the institutional framework of the European Union that now “expressly permits Union bodies, offices and agencies to adopt acts of general application”. In line with this ruling, there may be room for the EU legislator to allot rule-making powers to the DPAs.

5. Enforcement in the US: An Alternative System with a Strong Role for the FTC in Consumer Privacy

A system of independent DPAs does not exist in all democratic countries. The US has a different system, without independent supervision as an essential component of data


\textsuperscript{1707} Vos in: Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014.

\textsuperscript{1708} Case 98/80, Romano, EU:C:1981:104.

\textsuperscript{1709} As argued by the Council in Case C-270/12, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council, EU:C:2014:18, at 60 of the ruling of 22 January 2014.

\textsuperscript{1710} Case C-270/12, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council, EU:C:2014:18, at 65-66.
protection, contrary to the European Union and a large number of other Western countries, where a system of independent supervision exists. This systemic difference does not necessarily have a background of legal or constitutional principle, but may have been the result of opposition in the administration. Earlier drafts of the US Privacy Act (1974) contained a Federal Privacy Board. Opposition by administrative forces is mentioned as the main or even the sole reason for deleting this provision.

In the private sector, the most visible enforcement body is the Federal Trade Commission (FTC), which uses its authority against unfair or deceptive practices in the area of consumer privacy. Enforcement by the FTC encompasses the enforcement of some sectoral federal privacy laws, such as the Fair Credit Reporting Act (FCRA) and the Children’s Online Privacy Protection Act of 1998 (COPPA). The FTC also had enforcement authority on the basis of the Safe Harbor Agreement between the US and the EU, which the Court of Justice declared invalid in *Schrems*. This agreement provided for an enforcement mechanism with a key role for the FTC. The role of the FTC comes closest to the role of a data protection authority in the European Union.

The FTC adopts a wide and flexible strategy to privacy and data protection that focuses, to a large extent, on self-regulatory mechanisms. This strategy evolved from an approach based on the implementation of the Fair Information Practice Principles in the privacy policies of companies to a more harm-based approach.

---

1711 See Section 1 above.

1712 For an overview, Monika Kuschewsky (General Editor), Data Protection & Privacy, Jurisdictional Comparisons, Second edition 2014, Thomson Reuters.


1717 15 U.S.C § 1681 et seq.


1723 See below, Substantive standards of protection.

In recent years the FTC initiated enforcement actions against some of the big internet companies, with Google and Facebook as the most significant examples. In connection to its enforcement work, the FTC also assumes a role in policy development and actively promotes self-regulation. The FTC also calls on Congress to consider enacting baseline privacy legislation.

FTC enforcement is described by several scholars as a big success factor of protection in the US, delivering “privacy on the ground”. Emphasis is given to the magnitude of financial penalties, as well as to forward-looking injunctions. An example is the imposition of periodic audit requirements on companies that have violated privacy rules. These requirements may stay in force for 20 years and contain high civil penalties, in case a company does not comply with the requirements. Others point at the flaws in FTC enforcement, because of limitations in scope – for example, the FTC does not have competence as regards the financial sector – or because the FTC does not persist in following up on its injunctions. This perceived lack of persistence prompted the Electronic Privacy Information Center (EPIC) to establish an entire practice to incite the FTC into action.

The authority of the FTC to protect the consumer does not extend to the public sector. Here, enforcement of privacy and data protection is essentially organised by introducing checks and balances within organisational entities. Privacy offices within federal ministries headed by chief privacy officers play an important role in this system. External enforcement is not provided for. An exception is to a certain extent the Privacy and Civil Liberties Oversight Board, an independent agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007.

6. The DPAs as a New Branch of Government: Non-Majoritarian Expert Bodies, Different but Similar to EU Agencies

Independent DPAs as new branches of government, to be distinguished from autonomous agencies

---

1725 This is well described by Julie Brill, “Bridging the divide”, in: Hijnans and Kranenborg, Data protection anno 2014: how to restore trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), pp. 179-190.
1728 See David C. Vladeck, “A U.S. Perspective on Narrowing the U.S.-EU Privacy Divide”, in: Artemi Rallo Lombarte, Rosario García Mahamut (eds), Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime, at II.
1729 See: www.epic.org, on FTC complaints. See also Rotenberg in Privacy in the Modern Age, The Search for Solutions, Marc Rotenberg, Julia Horwitz, Jeramie Scott (eds), at 10-13.
1730 See: https://www.pclob.gov/.
The analysis starts from the premise that DPAs are a new branch of government that complement the traditional *trias politica* and, at the EU level, the institutional balance. They are independent authorities with constitutional status, with tasks attributed directly by the Treaties and not through delegation by the institutions.

The independence of DPAs distinguishes them from EU agencies, which operate in an autonomous way but not as independent bodies similar to DPAs. An important difference is that, contrary to EU agencies which exercise their tasks based on the basis of delegation, the DPAs are not subject to preferences of the executive branch of government. They are not legally subordinated to government.

More generally, DPAs should be distinguished from agencies in the sense of agencies that are “semi-autonomous organisations that operate at arm’s length of government in order to carry out public tasks […] relatively autonomously”. This distinction is in line with the argument that the term independence, applied to EU agencies, is confusing or even misleading and that it would be better to state that agencies operate – to a certain extent – in an autonomous manner. Although the difference between independence and autonomy may be semantic it is useful for understanding of the difference between DPAs and EU agencies. This is the reason why this chapter in some places uses the term autonomous in relation to EU agencies. It does not mean that in our view the term independence would not be justified in relation to agencies.

*The example of electronic communications: two main differences between the regulatory authorities and DPAs*

Autonomous or independent authorities exist also in other domains related to the internet and communications, both at the EU level and at the national level, with a cooperation mechanism between the authorities. A relevant example is the area of electronic communications, where national regulatory authorities play a central role, with the Body

---

1731 Van den Bergh (1952) already takes the view that the trias politica should not be understood as a static concept, requiring a strict separation between the three powers, but moreover reflects the need for checks and balances. Adding a new branch of government would be in line with this view, Bergh, G. van den, 1952, “Montesquieu en het Staatsrecht”, in: Verzamelde Staatsrechtelijke opstellen, Alphen aan den Rijn: Samsom.


1735 Other authors, such as Ottow, qualify agencies as independent, A.Ottow, Market & Competition Authorities, Good Agency Principles, Oxford University Press 2015.


of European Regulators for Electronic Communications (BEREC) fulfilling a mainly consultative role.

These national regulatory authorities (NRAs) have intervention powers against telecommunications operators with significant market power. The authorities have to be independent, but the requirements for independence differ significantly from independence requirements applicable to the DPAs. The focus is on the independence of the parties on the market they supervise, with a view to ensuring the impartiality and transparency of the decisions of the regulatory authorities. This is a functional autonomy. Moreover, the NRAs “should be in possession of all the necessary resources in terms of staffing, expertise and financial means, for the performance of their tasks”.

However, the independence or autonomy from the political arena – Lavrijssen & Ottow call this political independence – is less evident. These authors refer to practices within the OECD, where authorities should on the one hand be free to act without intervention from the executive, but on the other hand are bound by general government policy. A certain level of political autonomy is required in the area of electronic communications, ensuring that it is the regulatory authorities and not the governments that balance the objectives of the relevant instruments of EU law. However, this does not preclude the national legislature from acting as a regulatory authority, provided it meets the requirements of competence, independence, impartiality and transparency, and its decisions are subject to appeal.

There are two main differences between the regulatory authorities in the electronic communications sector and the DPAs. First, the regulatory authorities in the electronic communications sector are supposed to respect general government policies, which includes guidance by the Commission laid down in instruments of soft law, such as recommendations

---

1743 Case C-389/08, Base and Others, EU:C:2010:584, at 28.
1747 Case C-389/08, Base and Others, EU:C:2010:584, at 30.
and opinions, which under Article 288 TFEU do not have binding force.\textsuperscript{1748} By contrast, the DPAs do not have to respect this type of guidance, since that would not be in line with the independence of “any direct or indirect external influence on the supervisory authority”.\textsuperscript{1749}

Second, the requirements of what constitutes institutional independence are less strict. Article 3(2) of Framework Directive 2002/21\textsuperscript{1750} mentions legal distinctions and structural separations from other government entities, but these distinctions and separations must be made with entities that have – possibly – conflicting policy goals, for instance in a situation where a Member State has some ownership or control over a market party. As said, it is not even excluded that the national legislature acts as a regulatory authority. This is not comparable to the case law on DPAs where the Court of Justice of the European Union is strict in respect of any institutional interrelationship,\textsuperscript{1751} as will be explained below.

Finally, electronic communications is not the only area linked to the subject of this study where tasks are allotted to autonomous agencies. Another example is the area of consumer law, where national authorities are active and there exists a cooperation mechanism of national authorities responsible for the enforcement of consumer protection laws.\textsuperscript{1752}

\textit{DPAs: two main similarities with other non-majoritarian expert bodies}

Despite these differences DPAs display similarities with other non-majoritarian expert bodies, such as agencies at the European as well as at the national level. The roles of the DPAs fit within a more general trend of assigning certain public tasks to bodies composed of experts, and are in substance quite similar.\textsuperscript{1753}

Non-majoritarian\textsuperscript{1754} expert bodies – the word expertocracy\textsuperscript{1755} is used – play an important role in modern governance. Vibert describes this phenomenon as the rise of the unelected.\textsuperscript{1756}

\begin{footnotesize}
\begin{enumerate}
\item Case C-518/07, \textit{Commission v Germany}, EU:C:2010:125, at 19. It is in this context remarkable that the Commission wished to address the consequences of the ruling in Schrems “with clear guidance for national data protection authorities on how to deal with data transfer requests to the U.S., in the light of the ruling”, statement of First Vice-President Timmermans, \url{http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm}. \textsuperscript{1750}
\item See mainly Case C-614/10, \textit{Commission v Austria}, EU:C:2012:631.
\item E.g., by comparing the roles of DPAs mentioned in Section 4 with the roles of agencies, as listed by A. Ottow, Market & Competition Authorities, Good Agency Principles, Oxford University Press 2015, at 26.
\item E.g., in the annotation to Case C-518/07, \textit{Commission v Germany}, on the independence of data protection authorities by Jiří Zemánek, CMLR 49 (2012), 1755–1768, at 1756.
\item F. Vibert, \textit{The Rise of the Unelected}, Democracy and the New Separation of Powers, Cambridge University Press. His book and its title served as inspiration for this chapter. For the purposes of the chapter we assume that the main institutions of the EU (European Parliament, Council and Commission) do not qualify as unelected.
\end{enumerate}
\end{footnotesize}
In the EU context these unelected public bodies are usually indicated as agencies, and the trend is sometimes called ‘agencification’. Also the term regulatory agencies can be mentioned, reflecting a trend in the European Union to give agencies more regulatory tasks. This is the trend in the financial sector in reaction to the financial crisis, but the trend also extends to other areas. In the EU context the number of EU agencies has grown exponentially over recent years. Currently over 40 agencies exist. The most important similarity between DPAs and EU agencies is that they are both non-majoritarian expert bodies exercising public tasks.

A second similarity between DPAs and EU agencies is that they both operate as expert bodies in between the EU and national level. The DPAs are mostly national authorities operating within the general framework of EU law, deriving their position from both primary and secondary EU law, whereas the EU agencies are European bodies, but with a strong link to the national level.

These two similarities justify discussing the EU agencies in connection with DPAs. Of course, it would also make sense to include national regulatory agencies in the discussion, since in many instances they also operate as expert bodies in between the EU and national levels. The focus on EU agencies is justified by the perspective of this study, which is EU law.

In short, although DPAs – as follows from the case law of the Court of Justice on the independence of DPAs – should be clearly distinguished from EU agencies, a reflection on the EU agencies is relevant, if only because of the similarities. It is for these reasons that we include a general theory on expert bodies, a theory that in the EU context was developed mainly in relation to EU agencies.


Expert bodies with regulatory or supervisory tasks are a phenomenon that first appeared in Europe after the Second World War, with the first independent competition authorities. Schütz mentions the UK and Germany as the first European countries establishing these authorities. Philip Schütz; (2012): Comparing formal independence of data protection authorities in selected EU Member States,
However, these bodies had already existed for a longer period in the United States. The Interstate Commerce Commission, established in 1887 and becoming independent in 1889, is seen as the first independent authority.\textsuperscript{1766} The Federal Trade Commission, that plays an important role in the enforcement of privacy and data protection, was created in 1914.\textsuperscript{1767} This is remarkable, because in the United States the separation of powers between the executive, the legislative and the judiciary branch is stronger than in many other western democracies, although in the United States, too, functions are shared between the branches of government and checks and balances between the branches are a constitutional principle.\textsuperscript{1768} Experiences in the United States enable a better understanding of the constitutional position of bodies of experts.\textsuperscript{1769}

Currently, in a significant number of areas public tasks are exercised by unelected bodies of experts. This tendency is normally justified by the notion that those bodies have the expertise needed to act in complex areas of government action, taking into account facts and estimates in an effective way. They are better equipped than elected bodies for certain tasks, also because of the distance from the political discourse. Cost-effectiveness also plays a role.\textsuperscript{1770} The Court of Justice of the European Union justified giving public tasks to unelected bodies for reasons of expertise in \textit{United Kingdom of Great Britain and Northern Ireland v European Parliament and Council}\textsuperscript{1771} in relation to the financial stability of the Union. The Court accepted that powers of intervention were given to unelected bodies, precisely because of their professional expertise and their cooperative working methods. Commentators argue that faith in the power of technical expertise is an important source of legitimation of unelected bodies of experts.\textsuperscript{1772}

The contribution of expert bodies is providing citizens and companies with a predictable and stable environment where their rights or interests are protected in an adequate way. These bodies should also counterbalance the declining trust of citizens in the competence of government to effectively govern our complex societies, with the developing information society as a good example. This declining trust also has to do with the functioning of our democracies where – as Schütz argues – an important incentive for politicians is success in

\textsuperscript{1766} The Political Accountability of EU Agencies: Learning from the US Experience, (dissertation Maastricht, 2014), at 180-182.
\textsuperscript{1767} http://www.ftc.gov/about-ftc/our-history.
\textsuperscript{1769} Further read: M. Scholten The Political Accountability of EU Agencies: Learning from the US Experience, (dissertation Maastricht, 2014), at Chapter 3.
\textsuperscript{1771} Case C-270/12, \textit{United Kingdom of Great Britain and Northern Ireland v European Parliament and Council, EU:C:2014:18}, at 85.
\textsuperscript{1772} Schütz, with a reference to G. Majone, Philip Schütz; (2012): Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper, ECPR Standing Group on Regulation & Governance (Biennial Conference) <4, 2012, Exeter, at 5.
the next elections, so that they are not willing to commit to long-term solutions.\textsuperscript{1773} Shapiro formulates a paradox: new governmental bureaucracies are created – independent, unelected and endowed with specific tasks – as the result of the withdrawal of public trust in government bureaucracies.\textsuperscript{1774}

This does not mean that the rise of unelected expert bodies is unproblematic. The most obvious challenge – how to ensure democratic accountability – will be discussed below.\textsuperscript{1775} However, there is more to it. If various independent public bodies come up with contradictory solutions to similar social issues,\textsuperscript{1776} this will not enhance trust in government. Trust will also not grow because of the elitist nature of governing through independent bodies,\textsuperscript{1777} leaving decision-making to experts without scrutiny by elected parliaments. It must also be ensured that leaving decision-making to unelected expert bodies avoids the risk that these bodies act in a non-controllable and arbitrary manner.\textsuperscript{1778}

\textit{Are expert bodies a new branch of government?}

Expert bodies are public authorities outside the classic hierarchical administration and more or less independent of the government. Although constitutional theory is based on the presumptions of a separation of powers and on the level of the European Union on the presumption of a closed system of institutional balance, there is a trend of giving tasks to unelected expert bodies. The recognition of these bodies is also growing, sometimes even as new branches of government, with their own sources of legitimacy. EU agencies are the common illustration of these trends.

There are roughly two approaches to looking at the constitutional position of expert bodies. The first approach is to consider expert bodies as part of the executive branch, but with an independent position subject to certain safeguards. The second approach is to consider expert bodies as not being part of one of the traditional branches of government, namely the legislature, the executive, and the judiciary. They do not fit within the traditional \textit{trias politica}, as described by Montesquieu, with a separation of powers and a system of checks and balances between those powers,\textsuperscript{1779} but are a separate branch of government.\textsuperscript{1780}

\textsuperscript{1773} Schütz, equally with a reference to G. Majone, Philip Schütz; (2012): Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper, ECPR Standing Group on Regulation & Governance (Biennial Conference) <4, 2012, Exeter, at 5.
\textsuperscript{1775} In Sections 13 and 14.
\textsuperscript{1776} As Shapiro formulates, where government speaks with many independent voices; Shapiro, Independent agencies, in: Paul Craig and Grainne de Burca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 117.
\textsuperscript{1778} As stated by M.Busuioc & M. Groenleer, in Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, at 175.
\textsuperscript{1779} Baron de Montesquieu, De l’esprit des lois, 1748.
\textsuperscript{1780} In this sense F. Vibert, The Rise of the Unelected, Democracy and the New Separation of Powers, Cambridge University Press, as explained below.
The first approach – independent regulatory agencies as part of the executive – represents how these agencies are positioned in the United States, and also how – at first sight – they seem to fit into the constitutional framework of the Union.

In the United States independent regulatory agencies – with the Federal Trade Commission as an example – are part of the executive, but have a certain independence from the President, for instance in relation to the appointment and removal of their members and in the exercise of their functions that is not (or not fully) subject to executive orders. A typical characteristic is that the members should be selected from both political parties.

Within the European Union, the legal order is based on an institutional balance that does not include a strict separation of powers, but determines the way in which the various duties are shared between the institutions. According to the Meroni case law, it is a closed system and a fundamental guarantee granted by the Treaty. If one takes the closed system as a starting point, there is little room for introducing expert bodies as a separate branch. The same line is taken in the position of the Commission relating to EU regulatory agencies: these agencies are required to be actively involved in exercising the executive function. This allows the Commission to focus on its core tasks. In this view, the agencies primarily exercise tasks of the Commission, through delegation. A further argument against regulatory agencies as a separate branch can be drawn from the limitations imposed on the delegation itself in Meroni, in which delegation of discretionary powers to others was prohibited as this would render the EU legal order based on an institutional balance ineffective.

This being said, there is – as was explained above – a different approach for considering the constitutional position of expert bodies, the approach taken by Vibert. He proposes viewing unelected bodies – expert bodies, agencies, regulators – as a separate branch of government. As such, they do not derive their legitimacy from the other branches of government, as agents vis-à-vis a principal. The position of these bodies can be described as complementing the traditional structure of the trias politica. They should even be competent to supervise these other government branches within the traditional trias politica.

1782 The ‘bipartisan requirement’.
1783 According to Craig, the institutional balance, as a concept, is even opposed to the strict separation of powers. Paul Craig in Paul Craig and Grainne de Burca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 41-42.
1784 Case 9/56, Meroni, EU:C:1958:7, at 152.
1785 The Court states: “the balance of powers [which] is characteristic of the institutional structure of the Community a fundamental guarantee granted by the Treaty in particular to the undertakings and associations of undertakings to which it applies.
1787 Case 9/56, Meroni, EU:C:1958:7, at 152.
For Vibert, the starting point is that expert bodies do not pose a threat to our democratic system. According to us, they may even strengthen long-term policy perspectives in our democracies, thus filling a current void. The establishment of these bodies must therefore be considered from a positive angle, as a development enhancing the effectiveness of governments in a legitimate way.

This approach is attractive, in particular where the tasks of the expert bodies are directly attributed by virtue of primary EU law, which is the case for the DPAs. Their tasks are not delegated to them by the EU institutions. Moreover, one of the tasks of the DPAs is the control of the executive branch of government, which is not easily reconciled with considering DPAs as part of the (same) executive. Furthermore, there is a need for additional methods of oversight, in view of the loss of control over information in the internet society.\footnote{It was this lack of control that did trigger this study.}

The approach of Vibert is not only inherently attractive, but it might also be in line with the current state of EU law, even in relation to EU agencies. First, despite Meroni the prohibition of delegation of discretionary powers is not so strict. Second, the position adopted by the Commission on the regulatory agencies is not uncontested. Craig argues that the Commission’s concerns are based on the impact of agencies on the unity and integrity of its own executive function.\footnote{Craig in Paul Craig and Grainne de Burca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 68.} Third, the constitutional structures of the EU are based on an institutional balance, but they do not provide for independent expert bodies as part of the executive function of the Commission. Fourth, the institutional balance is not a static notion, but it develops over time. When Meroni was decided in 1958 the institutional balance was mainly a balance between the Commission and the Council, at a time where the European Parliament did not have real powers.\footnote{Further read: Craig in Paul Craig and Grainne de Burca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, Chapter 3.}

Against this background it is worthwhile presenting some essential elements of the theory of Vibert in this study. In this theory, a new branch of government would make sense because of flaws in our existing democratic systems, caused by information asymmetries\footnote{E.g., in Case 294/83, Les Verts v Parliament, EU:C:1986:166.} and because governmental actors have the wrong incentives to inform citizens and to act. Governmental actors avoid blame and, related to this, their main concern is seeking re-election. This diminishes the trust that individuals have in their governments.

The authorities within this new branch of government could be instrumental in restoring trust,\footnote{F. Vibert, The Rise of the Unelected, Democracy and the New Separation of Powers, Cambridge University Press, at 88-94.} using their independence and expertise to speak with authority within their

\footnote{F. Vibert, The Rise of the Unelected, Democracy and the New Separation of Powers, Cambridge University Press, gives, at 43-44, a range of arguments relating to knowledge and information, that is not repeated here.}
respective fields, and to solve problems and deal with conflicts of interest. However, there is also a downside from a democratic perspective. Where the authorities speak with authority, this may weaken the authority of the elected politicians. Moreover, their roles under the rule of law are not always clear and it is also not always clear how their findings are used in the political process.

Trust could be enhanced if the authorities were to operate within a context of checks and balances. Independence of these authorities implies that a complete separation of powers does not exist. The authorities cooperate within a constitutional framework with the traditional branches of government.

Checks and balances are part of this cooperation. A first aspect is the appointment of the members of the authorities. The right incentives should exist to take expertise and independence into account and to avoid purely political appointments. A second aspect relates to arrangements on working methods and procedures of the authorities, such as peer review or impact assessments. They should ensure that the authorities perform their tasks in an objective manner, based on the highest quality standards in the field.

A third aspect is the most complicated, the delimitation of responsibilities with elected bodies. It is argued that unelected bodies have an advantage in making empirical judgements, whereas elected bodies should make social or ethical judgements. However, this distinction is not fully clear, and – more importantly – it is an explicit task of some expert bodies to make social or ethical judgements. As exemplified by this study, DPAs are not in a position to make decisions on privacy and data protection, based purely on empirical facts.

Another delimitation relates to the adoption of legislative acts, which may be considered a task that is exclusively attributed to the legislative branch and may not be delegated to non-elected bodies. Under EU law, there is no strict prohibition of delegation of powers to adopt acts of general application, as was clarified by the Court of Justice in United Kingdom of Great Britain and Northern Ireland v European Parliament and Council. However, this does not necessarily mean that DPAs should be empowered to adopt legislative acts.

**DPAs are a new branch of government: towards good governance**

---

1800 This is not addressed by Vibert.
1801 Case C-270/12, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council, EU:C:2014:18, at 65.
This section recognised the differences between (EU) agencies and DPAs – based on the example of electronic communications – and subsequently focused on the similarities, since EU agencies and DPAs are both expert bodies operating in between the European Union and the Member States. Based on the theory of Vibert we will qualify the DPAs as a new branch of government.

As a new branch of government, the DPAs must act within the limits of their competence in accordance with requirements of independence, effectiveness and accountability. These requirements for governance under EU law are explained in the next sections.

Similar requirements have been developed for good governance of agencies. We mention two sources. Ottow distinguishes five Principles of Good Agency Behaviour with the acronym LITER (legality, independence, transparency, effectiveness and responsibility).1802 The analysis in the next sections follows these principles, although in a reworded fashion, where transparency and responsibility are subsumed jointly under the heading ‘accountability’.

The OECD developed seven Best Practice Principles for Regulatory Policy.1803 These are: role clarity, preventing undue influence and maintaining trust, decision-making and governing body structure for independent regulators, accountability and transparency, engagement, funding and performance evaluation. Section 4 of this chapter on the competences of the DPAs discussed their ‘legality’ or ‘role clarity’, in the wording of the sources just mentioned.

8. **EU Agencies and DPAs are Expert Bodies with a Hybrid Position in between the EU and National Levels**

At first sight, because DPAs derive their position from primary law their legitimacy is less controversial than that of EU agencies. However, certain arguments to the contrary also seem to be valid. We mention two of these arguments. First, the protection of individuals’ fundamental rights is a core task of national jurisdictions that should not be delegated to the European Union1804 and even less to unelected bodies established by EU law. Second, the requirements of independence of DPAs under the case law of the Court of Justice of the European Union are so strict that they prevent Member States from keeping any control over the DPAs. An illustration of the latter is the participation of representatives of Member States’ governments in the management boards of EU agencies, as compensation for their

---

1804 See on this Chapter 4 of this study.
loss of control.\textsuperscript{1805} This participation is meant to guarantee participation of the Member States in the agencies,\textsuperscript{1806} but is difficult to reconcile with the position of DPAs.

Both the EU agencies and the – in principle, national – DPAs exercise tasks as unelected expert bodies under EU law, but exercise their tasks with close links to the national jurisdictions. They all have a hybrid position in between EU law and national law. However, the origin of the EU agencies and the national DPAs is different, and as shown below, the trend is different.

EU agencies are EU bodies established under EU law. They operate within the EU legal order, have legal personality under EU law and their decisions are subject to review by the Court of Justice. EU agencies exercise tasks delegated to them under a specific instrument of secondary EU law. However, in return, the Member States have ensured that national influence is retained, for instance because representatives of the governments of the Member States participate in the management boards of agencies.\textsuperscript{1807} Another practice is that EU agencies cooperate closely with their counterparts at the national level, and that their position is characterised as \textit{primus inter pares} and not as a hierarchical relation.\textsuperscript{1808}

A specific and more recent phenomenon is the tendency to develop EU agencies out of the network of national supervisory authorities. The national regulators play a dominant role in the management.\textsuperscript{1809} These EU agencies, operating within the EU legal order, are clear examples of the hybrid position as referred to above.\textsuperscript{1810} The Body of European Regulators for Electronic Communications (BEREC)\textsuperscript{1811} is also interesting in this respect. In terms of organisation, BEREC embodies a compromise between European and national interests. BEREC consists of a network of national authorities and is supported by an office that is an EU body with legal personality.\textsuperscript{1812} However BEREC itself is a body of national regulators and is not an EU body. It is qualified as a “European network plus”.\textsuperscript{1813}

\begin{thebibliography}{9}
\bibitem{1805} Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, e.g., the contributions of Vos, at 34, and Ottow, at 135.
\bibitem{1806} Joint Statement and Common Approach of the European Parliament, the Council of the EU and the European Commission on Decentralised Agencies of 19 July 2012.
\bibitem{1807} In section 9. Further read, Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, e.g., the contributions of Vos, at 34, and Ottow, at 135.
\bibitem{1808} Vos in: Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, at 45.
\bibitem{1811} See on BEREC also Chapter 8, Section 6 of this study.
\end{thebibliography}
DPAs are national bodies established under national law, but once established, they exercise the tasks attributed to them by primary EU law. They operate within the national legal order, have a legal status under national law and their decisions are subject to review by national courts. However, they derive their position to a large extent from EU law and they exercise tasks attributed to them under primary EU law and elaborated in (secondary) EU data protection law. Currently, the Member States retain influence in the implementation of EU law, as concerns the organisation, the powers and the duties of the DPAs. This influence will be significantly reduced under the General Data Protection Regulation. However, the case law of the Court of Justice confirms that even under present law any influence on the performance of the tasks and duties of DPAs is prohibited.

In short, there is a tendency to give national interests a stronger say in the functioning of EU agencies that corresponds to the general trend in the European Union to pay more attention to subsidiarity. However, we also see an opposite tendency as far as DPAs are concerned. They are national authorities. At least the earlier DPAs were the product of national constitutional traditions, but step-by-step the national autonomy in relation to DPAs has diminished. This started with Directive 95/46. The case law of the Court was a further step, and this will be followed by the General Data Protection Regulation. Of course, the constitutional status of data protection after the entry into force of the Lisbon Treaty plays a role as well.

A final remark relates to a conclusion by Thatcher. He notes that in areas where Member States created national regulatory authorities, those national authorities resisted a strong EU agency. It remains to be seen whether this same behaviour will be observed in the area of privacy and data protection. A signal that this would indeed be the case can be observed in the position of the Article 29 Working Party on the institutional structure of its foreseen successor, the European Data Protection Board. The Working Party – consisting of all national DPAs as well as the European DPA, the EDPS – opposes the Commission Proposal for a General Data Protection Regulation, which puts the EDPS forward as a permanent vice-chair and is reticent as regards the possible role of the EDPS as secretariat of the new Board.

1815 Thatcher concludes that the EU adopted the agency form (by creating more agencies), but not yet the reality of agency governance, Mark Thatcher, The creation of European regulatory agencies and its limits: a comparative analysis of European delegation, Journal of European Public Policy 18:6 September 2011: 790–809, at 806.
1816 The examples of Germany and Sweden are illustrative, Philip Schütz: (2012): Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper, ECPR Standing Group on Regulation & Governance (Biennial Conference) <4, 2012, Exeter.
1818 Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals - WP 191 (23.03.2012), at 22.
9. Independence of DPAs under the Case Law of the CJEU: A Strong Requirement

On three consecutive occasions the Court of Justice of the European Union declared that national measures implementing Directive 95/46 did not meet the requirements of independence of DPAs under this directive. In Germany, the supervision on data processing by the private sector – a competence of the Länder under German law – was subject to state scrutiny.\(^{1820}\) As the Court stated, “the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities’ independent performance of their tasks”.\(^{1821}\) In Austria, the problem was not the independence of the decision-making process nor of the authority itself, but the fact that the authority (a collective body with mostly part-time members) depended on a managing member who was a career official and on a supporting office integrated in the Federal Chancellery.\(^{1822}\) The issue at stake in the case of Hungary was that a national law was adopted that replaced the existing DPA by a new authority.\(^{1823}\) The de facto result was that the Hungarian data protection commissioner – the sole member of the existing DPA – was replaced during his term of service.\(^{1824}\)

Arguably, Commission v Germany is the most important case in the context of this study, because the Court of Justice – for the first time and in a clear manner – defined the stakes of independence of the DPAs. These stakes were further specified in the two subsequent rulings. A summary of this case law is included in Schrems.\(^{1825}\)

The meaning of acting with complete independence: no external influence allowed

The Court of Justice underlined in Commission v Germany that under Article 28(1) of Directive 95/46 the DPAs should act with complete independence. The Court identified a double rationale for independence. It underlined that complete independence is needed to ensure effectiveness and reliability of the supervision,\(^{1826}\) thus contributing to its legitimacy. Based on the wording of the provision, and on the aims and the schemes of the directive,\(^{1827}\) this “implies a decision-making power independent of any direct or indirect external influence on the supervisory authority”.\(^{1828}\) In Commission v Austria, the Court further stressed that this is an autonomous interpretation, unrelated to the interpretation of the term court or tribunal of a Member State used in Article 267 TFEU.\(^{1829}\) Advocate General Mazak

---

1820 Case C-518/07, Commission v Germany, EU:C:2010:125.
1821 At 36 of the ruling.
1822 Case C-614/10, Commission v Austria, EU:C:2012:631, e.g. at 52 and 61.
1823 Case C-288/12, Commission v Hungary, EU:C:2014:237, e.g. at 59.
1824 For some further background: András Jóri, Shaping vs applying data protection law: two core functions of data protection authorities, International Data Privacy Law, 2015, Vol. 5, No. 2.
1825 Case C-362/14, Schrems, EU:C:2015:650, particularly at 40-43.
1826 Case C-518/07, Commission v Germany, EU:C:2010:125, at 25.
1827 Case C-518/07, Commission v Germany, EU:C:2010:125, at 29.
1828 Case C-518/07, Commission v Germany, EU:C:2010:125, at 19.
1829 Case C-614/10, Commission v Austria, EU:C:2012:631, at 40.
noted in his opinion\textsuperscript{1830} that the autonomous interpretation of the Court on the independence of DPAs may mean that a national authority could be regarded as independent under Article 267 TFEU, but does not fulfil the criteria of independence under EU data protection law, or, in other words, the requirements for independence of a DPA may be stricter than the requirements to qualify as court or tribunal.\textsuperscript{1831}

This interpretation should be further understood in the following way. What is decisive is not the formal status of the DPA,\textsuperscript{1832} but the freedom it enjoys in the exercise of its tasks. The emphasis on the acts of the DPAs may have to do with the wording of Article 28(1) of Directive 95/46, which does not state that the authorities should be completely independent, but that they should act as such.\textsuperscript{1833} Moreover, the case dates from before the entry into force of the Lisbon Treaty, and was based on Directive 95/46 and not on Article 16(2) TFEU and Article 8(3) Charter, which require that the authorities themselves are independent. In the subsequent cases, the Court of Justice observes that Article 28(1) of the directive derives from primary law,\textsuperscript{1834} but this did not lead to a modification of its position.

As far as a possible external influence on the exercise of the tasks is concerned, the Court is strict.\textsuperscript{1835} Most importantly, external influence is not only relevant when it originates from the entity under supervision, which can be a private company or a public authority. In a case relating to the supervision on the private sector no political influence over the decision-making process was acceptable, because it could hinder the independent performance of the task by the DPAs, whereas these authorities should remain above any suspicion of partiality. Hence, partiality is not required, suspicion is enough. What this means is well illustrated by an observation of the Court in \textit{Commission v Austria}, relating to a conceivable adaptation of the behaviour of the managing member of the Austrian authority, who used to be a career official. The prospects of promotion of this person could incite a form of ‘prior compliance’.\textsuperscript{1836}

The Court stated \textit{expressis verbis} that a government may have an interest in non-compliance by a non-public body with data protection law, and gave three examples why this could be the case.\textsuperscript{1837} A government may itself be an interested party, for instance because it engages in a public-private partnership, it may have an interest in the use of data, in particular for taxation or law enforcement,\textsuperscript{1838} and it may favour interests of economically important companies.

\textsuperscript{1830} Case C-614/10, \textit{Commission v Austria}, Opinion AG Mazak, at 25.
\textsuperscript{1832} The aim is not to grant a special status to the authorities, see at 25 of the ruling.
\textsuperscript{1833} This wording is chosen as a compromise formula, P. Hustinx in Reinventing data protection?, S. Gutwirth, et al. (eds), Springer 2009, at 132.
\textsuperscript{1835} Case C-518/07, \textit{Commission v Germany}, EU:C:2010:125, at 31-37 (in particular at 36).
\textsuperscript{1836} Case C-614/10, \textit{Commission v Austria}, EU:C:2012:631, at 51.
\textsuperscript{1837} Case C-518/07, \textit{Commission v Germany}, EU:C:2010:125, at 35.
\textsuperscript{1838} This links to what was said in this study on (government) surveillance.
Independence, according to the Court, is particularly important in light of the task of the DPAs, which consists of the balancing between the protection of the right to private life and the free movement of personal data. In other words, it is not only the need of effective privacy and data protection that counts, but also the balancing with other interests, with a broader scope than the rights to privacy and data protection.

The relation between the principle of democracy and the broad notion of independence

The Court of Justice ruled that the principle of democracy does not preclude independent public authorities outside the classic hierarchical administration. The DPAs must carry out their tasks free from political influence, but subject to judicial review.

However, and this is an essential addition: there should be some degree of parliamentary influence or, in other words, some degree of accountability towards political institutions. The Court gives an illustration of how this influence could be shaped. The management of the authorities may be appointed by the parliament, the powers may be defined by the legislator and reporting obligations to the parliament may be defined.

In Commission v Austria the Court dealt with a related issue, the influence of another political entity, namely the right of the Federal Chancellor to be informed of the work of the DPA. The right to information covered all aspects of the work of the DPA and was considered to be incompatible with the criterion of complete independence. The wording chosen by the Court suggests that it is not the right to information as such, but the extensive scope of this right, that provoked this conclusion. A contrario, a more limited right to information could ensure that the DPAs are to some degree accountable.

Four observations based on this case law

First, the Court of Justice mentioned effectiveness and reliability of supervision as an objective. Reliability is relevant in view of the subject matter of the supervision, the social sphere of individuals, which differs from supervision in the more technical, economic sphere where democratic legitimacy plays a less predominant role. The Court’s reference to reliability could also be understood as a confirmation that complete independence could be instrumental in restoring trust in governments in general, and in the European Union in particular.

---

1839 Case C-518/07, Commission v Germany, EU:C:2010:125, at 30.
1840 Case C-518/07, Commission v Germany, EU:C:2010:125, at 41-46.
1841 The Court also rejects arguments of the German government relating to the legal basis and to subsidiarity and proportionality, but these are not relevant for this part of the study.
1842 Case C-614/10, Commission v Austria, EU:C:2012:631, at 62-64.
1843 The importance of this accountability is underlined by the annotation of M. Szydlo on Case C-614/10, Commission v Austria, EU:C:2012:63, in CMLR 50 (2013), 1809-1826, at 1821-1822.
1845 As will be explained below in Section 13.
Second, the Court set a high standard for independence, also underlining the need for organisational distance to the executive. The way the Court explained the absence of any external influence implies that majoritarian bodies should not play any role in the exercise of the duties and powers of the DPAs. This standard reflects an earlier argument by Simitis (1987) who points at the risk that a DPA that is too close to government runs the risk of legitimising processing and new methods of information-gathering instead of controlling them. Still, there should be some degree of accountability towards political institutions, especially to parliaments and the judiciary.

This standard differs from the application of the notion of autonomy or independence in relation to EU agencies, where there is a practice that majoritarian bodies – the Commission, Member States and, where appropriate, the European Parliament – participate in the management boards of the agencies or where direct influence by the Commission is allowed in decision-making. Chiti even argues that this is a general difference between EU agencies and independent authorities. Independent authorities should be independent from private parties and from the political majority. In his view, the European Central Bank is the prime example, with strict safeguards on independence, as laid down in Article 130 TFEU. In comparison, the EU agencies are only independent to a limited extent.

Third, the Court underlined the task of the balancing of interests. Especially where various rights and values need to be balanced, there is a need for distance from majoritarian policy-making, to ensure a fair decision-making process. This is an important justification for independence. A need exists for the balancing of various interests, albeit within the mandate of the DPA relating to data protection. More generally, data protection is not an absolute fundamental right that prohibits the processing of personal data, but a right to fairness of processing, taking into account a range of different interests.

The Court mentioned the need for a fair balance between the protection of the right to private life and the free movement of personal data, but the need for balancing also relates to a range of other public interests, in particular the freedom of expression, security and transparency, all in a rapidly evolving technological environment. It could be argued that, in view of this case law, balancing between various interests – with a broader scope than the right to private life and the free movement of data mentioned in the ruling – is a task of DPAs. This raises

1846 And private organisations, but that is not relevant here.
1848 This is the model foreseen in the Joint Statement and Common Approach of the European Parliament, the Council of the EU and the European Commission on Decentralised Agencies of 19 July 2012.
1849 Further read, Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, e.g., the contributions of Vos, at 34, and Ottow, at 135.
1850 E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), 1395-1442, at 1399.
1851 And repeated in Article 7 of the Protocol (No 4) on the Statute of the European System of Central Banks and of the European Central Bank.
1852 As explained in Chapter 2 of this study.
1853 As mentioned in Case C-518/07, Commission v Germany, EU:C:2010:125, at 30.
the question how to ensure that the DPAs, as expert bodies in the area of data protection, take other interests into account.

The Court still used the wording in Commission v Germany\textsuperscript{1854} relating to balancing of interests, after the entry into force of the Lisbon Treaty.\textsuperscript{1855} This is remarkable since, generally, since the entry of the Lisbon Treaty the emphasis is on data protection as a fundamental right of the individual and no longer data protection as an instrument contributing to the free movement of data in the internal market.

To conclude, balancing of interests is part of the task of the DPAs and is relevant to their independence.

Fourth, the Court emphasised the importance of DPAs having discretionary powers and of them being in a position to make policy judgements, since the essence of their tasks is that they have to balance various interests, as underlined by the Court in Commission v Germany.\textsuperscript{1856} This is opposite to the Meroni\textsuperscript{1857} case law, where the Court emphasised that discretionary powers involving policy choices were not to be given to agencies. Only clearly defined executive powers – and not discretionary powers – could be delegated by the EU institutions, in the light of the institutional balance.\textsuperscript{1858}

In contrast, the powers and duties of DPAs, by nature, imply a high level of discretion. This confirms the special status of DPAs, different from EU agencies, although it must be admitted that the actual relevance of Meroni – a ruling of 1958 – in relation to agencies is disputed in legal literature.\textsuperscript{1859} Furthermore, the case law of the Court in relation to DPAs has developed, so that, presently, powers that involve discretion can to a certain extent be given to regulatory authorities.\textsuperscript{1860}

The emphasis in the case law on the balancing of various interests implies that independence is needed to avoid ‘prior compliance’. It also suggests that elected bodies – or more broadly: majoritarian institutions and, in particular, executive branches of government that depend on the support of a majority in parliament – may be ill-equipped\textsuperscript{1861} to deal with certain complexities of public policy, or more specifically law enforcement, in comparison with unelected bodies.

\textsuperscript{1854} The reference to the internal market in Case C-518/07, Commission v Germany, EU:C:2010:125, at 30, is made even more explicit in para. 50 of the ruling.
\textsuperscript{1855} In Cases C-288/12, Commission v Hungary, EU:C:2014:237, at 51, and C-362/14, Schrems, EU:C:2015:650, at 42.
\textsuperscript{1856} Case C-518/07, Commission v Germany, EU:C:2010:125, at 24.
\textsuperscript{1857} Case 9/56, Meroni, EU:C:1958:7, at 152.
\textsuperscript{1858} See on the Meroni doctrine: Vos in Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, at 40.
\textsuperscript{1859} See, e.g., E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), 1395-1442, at 1421-1424.
\textsuperscript{1860} Case C-270/12, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council, EU:C:2014:18 (on ESMA), ruling of 22 January 2014 and the Opinion of AG Jääskinen.
10. Independence of DPAs: An Analysis

Different degrees of independence under EU law, parallels with the ECB and with courts

Different degrees of independence exist. In the area of data protection the DPAs are subject to high requirements of independence. This was, as we have seen before, confirmed by the case law of the Court of Justice of the European Union\(^\text{1862}\) and it has a functional as well as an institutional component.\(^\text{1863}\) In the EU framework, this status of the DPAs can be best compared with that of the European Central Bank (ECB), which enjoys a high level of independence, as laid down in Article 130 TFEU.\(^\text{1864}\) Article 130 TFEU provides that neither the ECB nor national central banks shall seek or take any instructions from EU institutions or bodies, or from the Member States. Moreover, the EU institutions or bodies and the Member States undertake to respect this principle. This is also laid down in a concise manner in Article 282(3) TFEU: The ECB is independent in the exercise of its powers and EU institutions and bodies, as well as the Member States, shall respect that independence. As the Court stated in *Commission v European Central Bank*,\(^\text{1865}\) the Treaty seeks “to shield the ECB from all political pressure in order to enable it effectively to pursue the objectives attributed to its tasks”.

We are not claiming that the level of independence of DPAs is the same as that of the ECB, which operates in a totally different area of government intervention, but there is a similarity. The wording used by the Court of Justice in relation to DPAs prohibiting any direct or indirect external influence on the supervisory authority\(^\text{1866}\) implies that they “shall not seek or take any instructions”.\(^\text{1867}\) Moreover, the prohibition of any direct or indirect external influence on the supervisory authority implies a reciprocal duty. EU institutions and bodies as well as Member States should abstain from influencing DPAs.

Another similarity concerns the requirements for national courts and tribunals under Article 267 TFEU. These requirements determine which courts or tribunals can refer cases to the Court of Justice. Independence is one requirement and includes, amongst others, guarantees against dismissal or removal from office.\(^\text{1868}\) However, there is one difference. In *Dorsch Consult Ingenieursgesellschaft*,\(^\text{1869}\) the Court did not consider the fact that the organisational structure of a body was linked to the executive sufficient reason for denying its independence. Bodies called ‘mixed councils’ under Austrian law were admitted to refer cases to the Court, whereas the (former) Austrian data protection authority – also a mixed

---

\(^\text{1862}\) See, e.g., ruling of CJEU in Case C-518/07, *Commission v Germany*, EU:C:2010:125.

\(^\text{1863}\) See European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at II.8.

\(^\text{1864}\) And repeated in Article 7 of the Protocol (No 4) on the Statute of the European System of Central Banks and of the European Central Bank.


\(^\text{1866}\) Case C-518/07, *Commission v Germany*, EU:C:2010:125, at 19.

\(^\text{1867}\) Article 130 TFEU.

\(^\text{1868}\) Case C-54/96, *Dorsch Consult Ingenieursgesellschaft*, EU:C:1997:413, at 34-38.

\(^\text{1869}\) Case C-54/96, *Dorsch Consult Ingenieursgesellschaft*, EU:C:1997:413, at 34-38.
council under Austrian law – was not considered completely independent under Directive 95/46.\footnote{1870}

Despite this autonomous interpretation of data protection law there is a clear similarity with the case law relating to Article 267 TFEU. This is for instance illustrated by the reasoning of the Court in \textit{Syfait and Others}\footnote{1871} where it did not accept the independence of the Greek national competition authority (the Epitropi Antagonismou). The Court took into account that, despite the personal and operational independence of the members of this authority, there were no effective safeguards against undue intervention or pressure from the executive on those members. The Court also noted that “the Epitropi Antagonismou is not a clearly distinct third party in relation to the State body which, by virtue of its role, may be akin to a party in the course of competition proceedings.”\footnote{1872} So, the absence of sufficient guarantees against external influence, caused by the risk of the executive having specific interests, was a reason for declaring that a body did not fulfil the criteria of independence under Article 267 TFEU.

In contrast, the autonomy granted to EU agencies is different in character. The agencies do not enjoy a comparable high degree of independence. The ability of EU agencies to act can be subject to restrictions by majoritarian bodies. Courts are supposed to be independent from political preferences, whereas the agencies are part of the administration, loyal to government and acting on its behalf.\footnote{1873}

In any event, to the extent that agencies have tasks in relation to the functioning of the market, they are autonomous vis-à-vis market forces, but not vis-à-vis political majorities.\footnote{1874} A good example in this context is the participation of the governments of Member States in the management boards of EU agencies.\footnote{1875} One can argue that this is against the rationale of the existence of independent agencies. However, one can also argue that this makes sense, since agencies may be technocratic in character although they also may have to give value judgements on public interests that are, by their very nature, political. It also makes sense from the perspective of giving the Member States influence on the performance of technocratic bodies at EU level.\footnote{1876} To put it differently, where EU agencies act national powers are not only transferred to the European Union, with its alleged democratic deficit,\footnote{1877} they are actually being transferred to a technocratic body within the European Union. This

\begin{footnotesize}
\begin{enumerate}
\item Case C-53/03, \textit{Syfait and Others}, EU:C:2005:333, at 33.
\item Anna-Sara Lind and Jane Reichel, Administering Data Protection – or the Fort Knox of the European Composite Administration, \textit{Critical Quarterly for Administration and Law} (EuCritQ), 2014, 1, pp. 44-57, at 53.
\item See on this, Chiti, CMLR 46 (2009), 1395-1442.
\item Also the Commission and, where appropriate, the European Parliament participate in these Management Boards.
\item Further read: E. Vos in Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, at 29.
\item See on this Chapter 4, Section 10 of this study.
\end{enumerate}
\end{footnotesize}
justifies a certain limitation of the independence of these bodies and the maintenance of some political control.

**High degree of independence for DPAs, confirming their status as new branch of government**

As explained above, under EU law, the independence of DPAs is a constitutional requirement. The Court of Justice confirms that control by an independent authority is not only laid down in Article 28 of Directive 95/46, but that this requirement also derives from primary law.\(^\text{1878}\) This has two consequences: on the one hand, independence is an autonomous concept that cannot be restricted either by the EU legislator or by the Member States in their national laws, and, on the other hand, the European Union and the Member States are obliged to actively ensure the independence of the DPAs or, in other words, to give substance to the concept of independence.

Moreover, as was also explained before, this study argues that the DPAs – and certain other expert bodies – qualify as a new branch of government complementing the traditional separation of powers. The institutional framework of the European Union is based on the institutional balance, which is not a static notion.\(^\text{1879}\) We argue that DPAs, as far as they exercise control at the European level, also complement the existing institutional balance. Support for this argument can be found in the former Article 286 EC as the legal basis for the foundation of the EDPS.\(^\text{1880}\) Since the EDPS was also empowered to supervise the activities of the EU executive – the Commission is the clear example here – a separate constitutional position was needed. Merely integrating the EDPS into one of the existing institutions would not have been sufficient.\(^\text{1881}\) The Lisbon Treaty replaced Article 286 EC by Article 16 TFEU, which is formulated in more general terms and no longer provides for a specific legal basis of a European DPA. However, the general requirement of Article 16(2) TFEU also implies independent control of the EU institutions, which cannot be exercised by one of the institutions themselves. Hence, there must be a body supervising the institutions and complementing the institutional balance. A final remark in this context is that a European DPA is not amongst the EU institutions, listed in Article 13(1) TEU. This study considers this to be an omission in the Treaty on European Union.

The high degree of independence for DPAs has been specified by the Court in the three cases that were brought before it.\(^\text{1882}\) This independence of the DPAs is mainly limited by the judicial and political accountability described below.

However, guarantees for the independence of DPAs are not only the result of negative obligations of the European Union and national governments, they also imply positive

\(^{1878}\) Case C-614/10, *Commission v Austria*, EU:C:2012:631, at 36; Case C-288/12, *Commission v Hungary*, EU:C:2014:237, at 47. See also section 9.

\(^{1879}\) See Section 7 above.

\(^{1880}\) See also Section 3 above


obligations. The most obvious obligation is adopting legislation that enables complete independence. The European Union and national governments should also create the circumstances necessary for the establishment and functioning of independent authorities in practice. One example of this will be explored below.

The appointment of members of a DPA: a critical factor potentially influencing independence

One of the most critical factors potentially influencing the independence of DPAs is the way in which the members of a DPA are appointed. It is at this instance where majoritarian bodies may exercise their influence. In this context, too, checks and balances are essential. Scholten makes an interesting observation in respect of the appointment of members of independent regulatory agencies in the United States, which requires the common involvement of both the Congress and the President. A divided government may lead to a better outcome than a unified government where one party can advance its political candidates. Of course, there is an objection to this statement since a divided government may also lead to a deadlock, but in general ensuring the involvement of various points of view may provide an incentive to appointing suitable candidates.

Current and future EU law includes safeguards that must ensure that choices are based on the expertise and independence of the candidates for a function. The procedure foreseen for the appointment of the European Data Protection Supervisor serves as an illustration. Article 42 of Regulation 45/2001 requires, in the first place, the involvement of three institutions, the European Parliament, the Council and the Commission. In the second place, there are requirements giving the procedure a certain degree of transparency: the call for candidates is public, the list of candidates is public and the European Parliament is entitled to organise a public hearing which, in practice, it does. In the third place, Article 42 of Regulation 45/2001 requires the chosen candidate to possess specific qualities: his or her independence must be beyond doubt, he or she must have the experience and skills required to perform the job, and it is seen as an advantage if he or she is a member or has been a member of a national DPA. The General Data Protection Regulation contains similar wording.

However, the proposed regulation does not require the involvement of the various branches of government in the appointment procedure of national DPAs, which can be explained by the fact that appointment of the members of these national authorities is a task of the Member States, in accordance with the principle of national procedural autonomy. The Commission proposal allows appointment either by the parliament or the government. The

---

1884 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
1885 See mainly Article 3 of Decision No 1247/2002/EC of the European Parliament and of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor’s duties, OJ L 183/1
1887 Case C-93/12, Agrokonsulting-04, EU:C:2013:432, at 35
legislative resolution of the European Parliament limits this to an appointment by the national parliament.\textsuperscript{1888}

In the hypothesis that the DPAs are new branches of government in between the three traditional branches it would strengthen the position of the DPAs if all branches of government were involved in the appointment of members of DPAs. In any event, the discussion on the appointment of the DPAs has focused on the position of the legislative and the executive branch, whilst the possibility of a role of the judiciary branch in the appointment procedure has not been considered.

\textit{The DPAs have an obligation to safeguard their independence, under the principle of democracy}

As explained above, in \textit{Commission v Germany}\textsuperscript{1889} the Court of Justice underlined the relationship between independence of DPAs and the principle of democracy. It follows from this relationship that independence is not merely a negative obligation for elected bodies to refrain from influencing the DPAs, but that the DPAs themselves have – within a democratic society – an active obligation to preserve their independence. They should not allow any external influence in the performance of their tasks.

This active obligation is particularly important in view of the broad tasks of the DPAs, which are in many instances not performed in isolation, but in close contact with stakeholders, be they governments, representatives of the private sector or civil society. For example, as part of its enforcement activity, a DPA may advise a company on the measures it should take in order to comply with data protection law. If, in a later stage, an individual lodges a complaint with the DPA against the company in relation to these measures, the DPA must remain above any suspicion of partiality, as required by the case law of the Court. This is not evident, where the DPA was involved in designing the measure at stake.\textsuperscript{1890} The same could also happen at a more general level: where DPAs were initially involved with governments, representatives of the private sector and/or civil society in the design of codes of conduct or implementing measures, this may at a later stage (potentially) influence enforcement.

\textit{Independence in relation to effectiveness and accountability}

The Court of Justice underlined in \textit{Commission v Germany}\textsuperscript{1891} that there is a clear link between independence and effectiveness. Hence, this link supports the view that effectiveness can legitimise DPAs. This is the output legitimacy, explained in Chapter 4 of this study.\textsuperscript{1892}


\textsuperscript{1889} Case C-518/07, \textit{Commission v Germany}, EU:C:2010:125, at 41–46

\textsuperscript{1890} See also Chapter 6, Section 14 of this study.

\textsuperscript{1891} Case C-518/07, \textit{Commission v Germany}, EU:C:2010:125, at 25.

\textsuperscript{1892} See Chapter 4, Section 13.
DPAs do not escape accountability towards the elected parliaments. In *Commission v Germany*, the Court gave indications for the assurance of accountability. This need for parliamentary influence can be satisfied by the Member States under Directive 95/46, which leaves a wide discretion to the Member States as to the establishment and functioning of the DPAs. Under the General Data Protection Regulation this discretion will be significantly reduced, although the Regulation will allow for the appointment of the members of the DPAs by national parliaments. The EDPS opinion on the reform package suggests reinforcing the democratic guarantees by requiring a more systematic role for the national parliaments in the procedure for the appointment of these members. Moreover, the case law gives some further indication on ensuring accountability in a more general sense, since the Court does not preclude that governmental bodies have a right to be informed.

11. **Effectiveness of DPAs: A Presumed Lack of Effectiveness and the Struggle for Resources**

Under primary EU law, compliance with data protection rules shall be subject to the control of DPAs. Article 8(3) Charter and Article 16(2) TFEU imply that the control must not only be exercised in an independent manner, but that it also must be effective. This is the consequence of the principle of effectiveness under EU law. DPAs must be enabled to exercise the powers listed in Article 28 of Directive 95/46 in an effective manner.

The effectiveness of the DPAs is interrelated with their independence. As the Court of Justice of the European Union underlines, independence is intended to ensure the effectiveness of supervision. It thus qualifies independence as a precondition for effectiveness. This does not mean that independence alone guarantees effectiveness, nor that effectiveness is an element of independence. Effectiveness is a separate criterion that in any event requires that the DPAs have effective powers and that appropriate resources are made available.

Effectiveness is the second building block for a good functioning of the control by DPAs, in the same way as effectiveness is required for any government action. A democracy without adequate powers cannot function as a democracy and the case law of the Court of Justice constantly emphasises the principle of effectiveness as a cornerstone of EU law, including

---

1895 European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 236, with a reference to *Commission v Germany*.
1898 The powers listed in Article 28 are powers of investigation, powers of intervention, powers to hear claims and to engage in legal proceedings.
European administrative law\textsuperscript{1901} to which the DPAs are also subjected. For DPAs, effectiveness is an important \textit{raison d'être}. DPAs have added value, because they are expected to be an effective tool in the protection of personal data. Dimensions that are relevant in this context, in addition to powers or resources, are expertise and flexibility. The DPAs are small bodies, but their resources can all be used for data protection.

\textit{The presumed lack of effectiveness of DPAs}

At present, a presumed lack of effectiveness of DPAs is seen as a major deficiency of data protection in the European Union, with an emphasis on insufficiencies in the powers and resources of the DPAs.\textsuperscript{1902} Bamberger & Mulligan report that these “shortcomings are particularly acute with regard to regulatory adaptivity to new technological contexts”.\textsuperscript{1903}

Against this background it is not surprising that the need for the creation of more effective enforcement by DPAs is one of the main purposes of the proposal for a General Data Protection Regulation.\textsuperscript{1904} One of the main deficiencies the Commission identifies is the lack of effective supervision through regulatory authorities with sufficient powers, as well as insufficient guarantees for consistent enforcement. According to the Commission, the resources and the powers of the national authorities responsible for data protection vary considerably among Member States. In some cases, DPAs are unable to perform their enforcement tasks in a satisfactory manner. For these reasons, the Commission felt that national authorities need to be reinforced and their cooperation strengthened in order to guarantee consistent enforcement and, ultimately, the uniform application of rules across the European Union.\textsuperscript{1905}

Also the Fundamental Rights Agency of the European Union reported on the great variety as well as on deficiencies in powers and resources of DPAs.\textsuperscript{1906} As to powers, the Agency reports that, in certain Member States, the DPAs are not endowed with the full range of powers of investigation, powers of intervention and powers to hear claims and engage in legal proceedings. These are the powers referred to in Article 28(3) of Directive 95/46. Examples of deficiencies the Agency mentions relate to the lack of intervention powers, as

\begin{itemize}
  \item\textsuperscript{1901} See on this, e.g.: Harlow in Paul Craig and Grainne de Burca (eds), The evolution of EU Law, Second Edition, Oxford University Press 2011, at 447. On the principle of effectiveness in general: see Paul Craig and Grainne de Burca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at various places, e.g. at 223-237, in relation to remedies before national courts.
  \item\textsuperscript{1904} COM (2012), 11 final.
  \item\textsuperscript{1905} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, COM (2012), 9 final, pp 6-7.
  \item\textsuperscript{1906} Fundamental Rights Agency, Access to data protection remedies in EU Member States, 2013, at 4.2 and in Fundamental Rights Agency, Data Protection in the European Union, the role of National Data Protection Authorities, 2010, at 5.1.1.
\end{itemize}
well as the absence of the power to enter premises where personal data are processed without first obtaining a judicial warrant. Also limited sanctioning powers – for example, fines of a non-dissuasive nature – were reported, in combination with the absence of a practice of imposing sanctions. An example of limited sanctioning powers is a decision of the Sanctions Committee of the French DPA (CNIL), imposing a monetary penalty of 150,000 Euro on Google, because its privacy policy did not comply with French data protection law. This penalty is neither substantial nor dissuasive in view of the annual turnover of Google.

As a rule, sanction powers are restricted in view of the fact that the DPAs should be able to effectively enforce infringements by big internet companies. This is addressed in the General Data Protection Regulation, but in the meantime it is an obligation for the Member States implementing Directive 95/46 to ensure effectiveness, also by attributing appropriate sanctioning powers. After the entry into force of the General Data Protection Regulation, this obligation remains with the Member States, but will be subject to precise parameters set by EU law.

**Resources of DPAs**

The Fundamental Rights Agency reported on understaffing and a lack of adequate financial resources of DPAs, with the result that in many Member States the DPAs do not carry out all their tasks.

Article 47(5) of the proposed General Data Protection Regulation deals with resources and distinguishes between adequate human, technical and financial resources, premises and infrastructure. Member States shall ensure that adequate resources are provided, without giving indications how the adequacy of the resources can be measured. The legislative resolution of the European Parliament specifies that particular attention should be given to ensuring adequate technical and legal skills of staff. In its opinion on the reform package, the Article 29 Working Party suggested a mechanism for measuring the adequacy of financial

---


1910 An example of increased sanctioning powers can be found in The Netherlands. The Dutch DPA will be, as from 2016, empowered to impose administrative fines with a maximum of 810,000 Euro, Staatsblad 230 Wijziging van de Wet bescherming persoonsgegevens, 2015.

1911 A principle for funding is found in the OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing. http://dx.doi.org/10.1787/9789264209015-en, at 98: “Funding levels should be adequate to enable the regulator, operating efficiently, to effectively fulfil the objectives set by government, including obligations imposed by other legislation.”

1912 Fundamental Rights Agency, Data Protection in the European Union, the role of National Data Protection Authorities, 2010, at 5.1.1


1914 Article 47(5) and rectif 94 of the proposed General Data Protection Regulation

1915 Legislative Resolution of the European Parliament, Amendment 65, relating to rectif 94.
resources, which should consist of a fixed amount supplemented by an amount based on a formula related to the population of a Member State and its GDP.\textsuperscript{1916}

The allocation of resources starts with an adequate budget for the DPAs,\textsuperscript{1917} allowing for the attribution of sufficient equipment and staff. In \textit{Commission v Austria} the Court of Justice ruled that a sufficient budget is needed, but this does not require a separate budget.\textsuperscript{1918} Normally, the DPAs are (fully) funded by the public budget. An exception is the Information Commissioner’s Office in the United Kingdom, which is funded by fees levied from data controllers.\textsuperscript{1919} The responsibility for the public budget in a democratic society is a matter where involvement of democratically elected bodies is a \textit{conditio sine qua non} and where normally spoken the influence of DPAs is limited.

The available human resources – the members of the DPAs as well as the staff – must ensure an effective implementation of the powers. This requirement does not only have a quantitative aspect, but also a qualitative aspect. In \textit{Commission v Austria} the Court mentioned that resources – in particular equipment and staff – must be attributed in such a way that it does not prevent the DPAs from acting independently.\textsuperscript{1920} The way staff was attributed to the Austrian DPA did not guarantee that the staff would act in an independent manner. As observed before, the staff was composed of officials of the Federal Chancellery of Austria.

Furthermore, the expertise of the human resources must be guaranteed. In the preparatory documents leading to the proposed reform of the EU data protection framework, expertise did not appear as an important issue in relation to DPAs. Lack of expertise was not mentioned as a trigger for the reform of the EU data protection legislation. However, ensuring expertise within the DPA is essential, because it is the expertise that provides legitimacy. The Court did not state this explicitly in its case law on the independence of DPAs, but it confirmed this for the financial area, in \textit{United Kingdom of Great Britain and Northern Ireland v European Parliament and Council}.\textsuperscript{1921}

Finally, technical resources must be available, including premises and infrastructure.\textsuperscript{1922} These resources are not specifically addressed in this section of the study on the effectiveness

\textsuperscript{1916} Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals - WP 191, at 17.


\textsuperscript{1918} Case C-614/10, \textit{Commission v Austria}, EU:C:2012:631, at 58.


\textsuperscript{1921} Case C-270/12, \textit{United Kingdom of Great Britain and Northern Ireland v European Parliament and Council}, EU:C:2014:18, at 85.

\textsuperscript{1922} As mentioned in Article 47(5) of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
of DPAs. We just mention them to underline that various resources are needed for a DPA to enable it to operate in an effective manner.

12. **Effective Powers of DPAs, Proximity and the Developing Information Society**

**Member States must ensure effective powers**

The consequences of the principle of effectiveness for the powers of investigation and the powers of intervention of DPAs are that the Member States must ensure that these powers can be exercised in an effective manner. This is not an obligation that, under current law, can easily be quantified or challenged in legal proceedings. Article 28(3) of Directive 95/46 is not very specific. The Commission has not brought cases before the Court of Justice under the infringement procedure of Article 258 TFEU based on the argument that a Member State has provided insufficient powers to a DPA. However, the Court recognised that the absence of intervention powers is problematic when the processing is carried out outside the territory of the European Union.\(^{1923}\)

From the perspective of the individual who is entitled to – effective – protection the following elements are relevant, as a result of Article 16(2) TFEU and Article 8(3) Charter, read in combination with Article 28 of Directive 95/46. In the first place, when an individual (or an association representing him or her) lodges a complaint with the DPA the claim shall be heard and the complainant shall be informed of the outcome.\(^{1924}\) The claim can also relate to an act of a controller established in another Member State. A DPA may examine a complaint irrespective of the applicable law.\(^{1925}\) In the second place, Article 16(2) TFEU and Article 8(3) Charter require that individuals shall have effective access to remedies against breaches of data protection law, in line with Article 47 Charter. This follows from the very nature of the control, by DPAs, an essential component of the protection of individuals.\(^{1926}\) This presupposes ensuring remedies in national law, in accordance with the principles of equivalence and effectiveness.\(^{1927}\)

**Proximity of DPAs enhancing effectiveness**

Under Article 16(2) TFEU and Article 8(3) Charter, an individual may, under all circumstances, claim that the exercise of his or her rights is under the control of an independent authority. Member States should ensure that the procedures are put in place to guarantee protection by DPAs, in accordance with the principles of equivalence and effectiveness.

\(^{1923}\) Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* (C-293/12) and *Seitlinger* (C-594/12), at 68, and Case C-362/14, *Schrems*, EU:C:2015:650, at 44.

\(^{1924}\) Article 28(4) of Directive 95/46.


\(^{1926}\) See, e.g., Section 1 of this chapter.

effectiveness. The legal order of the Union is based on the notion that where competences are transferred to the Union, the Member States remain responsible for remedies being available in the national legal order.

The debate during the legislative procedure on the General Data Protection Regulation on what is referred to as proximity could be seen in this context. This debate related to the question whether proximity required that individuals are entitled to protection by the DPA within the Member State where he or she resides, or whether effective protection can also be provided by another DPA. Proximity is a specification of a basic principle of the Treaty on European Union, namely that decisions are taken as closely as possible to the citizen.

It could be argued that this control should be guaranteed by an authority of the jurisdiction where an individual has his usual residence, which would mean that the requirements of Article 16(2) TFEU and Article 8(3) Charter influence the functioning of the European composite administration in this specific area. Proximity is not a prerequisite for legal protection under EU law. What counts is the effectiveness of redress mechanisms. However, proximity could be an argument in support of effectiveness in an internet context, since it counterbalances forum shopping by big internet companies, choosing a Member State of establishment on the basis of the (lack of) enforcement capacity of its DPA.

Under the same argument that control should be guaranteed by an authority in the country of residence, current EU law permits forum shopping by big internet companies, choosing as Member State of its main establishment a country with a perceived low level of DPA enforcement. Vice versa, a DPA is not permitted to enforce data protection law, if an internet company chooses an establishment abroad, whilst targeting individuals within the Member State where the DPA functions.

The topic is illustrated by the enforcement actions of several national DPAs against Facebook. According to a press release of the Belgian DPA Facebook seems to claim that under Article 4(1)(a) of Directive 95/46 only the Irish DPA is competent to enforce the directive against it, as Facebook has its main European establishment in Ireland. Without prejudice to the correctness of the position of Facebook under Directive 95/46, the argument

---

1931 Article 1(2) TFEU.
1932 The interaction of individuals with the European composite administration in this area is mentioned in Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57, at 55.
1933 Further read, Opinion Legal Service Council, e.g. 18031/13 (19 Dec 2013, full version on lobbyplag.eu).
1934 As explained in Chapter 8, Section 12.
based on proximity could be made that an EU citizen who is directly affected by data processing of his personal data by Facebook would be entitled to protection by the DPA in the Member State where he or she resides, directly on the basis of Article 16(2) TFEU and Article 8(3) Charter.

**Effective DPAs in a developing information society**

This study started from the presumption that governments have lost control over societal developments, due to globalisation and technological developments, exemplified by big data and mass surveillance.

The European Union and the Member States have the obligation to ensure effective protection by DPAs, in a complex global and technological environment, and that, where needed, trust can be restored. Obviously, there is a budgetary restriction. Resources given to DPAs are part of the national budget – or in the case of the European Union itself, of the EU budget – and have to be balanced against resources spent for other public tasks.

The next issue is how – given restrictions in terms of resources – the authorities can be incentivised to ensure control in the most effective manner. Here we encounter a dilemma. As explained, the DPAs are given a high degree of independence because of the added value of having authorities with specific expertise and acting impartially, free from any external influence.\(^{1937}\) This independence does not only mean that they have discretion in solving cases before them, but also in setting priorities. The DPAs also claim that a wide discretionary power is needed to be effective, which means that selective approaches are seen as a guarantee for effective data protection.\(^{1938}\)

In other words, the DPAs are free to set their own agenda. There is one limitation, the complaint handling by a DPA.\(^{1939}\) Under Article 28(4) of Directive 95/46 a DPA “shall hear claims lodged by any person”. Furthermore, the “person concerned shall be informed of the outcome of the claim”. The obligation of a DPA to handle a complaint is the subject of the pending case *Rease and Wullems*.\(^{1940}\) The referring judge has asked the Court of Justice whether a DPA – in this case the DPA of the Netherlands – is free “to set priorities which result in such enforcement not taking place in the case where only an individual or a small group of persons submits a complaint alleging a breach of that directive”. In other words, is a DPA empowered to renounce from enforcement in a case that may be important for the complainant but not for society as such.

---

1937 Case C-518/07, Commission v Germany, EU:C:2010:125, at 19.
1939 In Case C-362/14, Schrems, EU:C:2015:650, at 53, the Court reiterates the importance of lodging complaint before a DPA.
1940 Case C-192/15, Rease and Wullems (pending).
The question is not so much whether an individual is entitled to an answer when he lodges a complaint, but whether the DPA is required to take any further action after a complaint is lodged. Hustinx pleads for a reasonable discretion of DPAs as to whether and how to deal with complaints. In essence, the issue is whether an individual is entitled to a remedy before a DPA as part of his fundamental right under Article 47 Charter, or that it suffices that he can invoke his right, alternatively, before a court.

This is an essential issue for the functioning of the relatively small DPAs, which could become paralysed if disproportionate resources have to be used for complaint handling. The ruling in Rease and Wullems could present an opportunity to resolve this issue, and at the same time provide clarity on the nature of the right to complain with the DPAs.

The DPAs are important actors under EU law in an area where trust in the capacity of governments to deal with fundamental developments in our societies in an effective manner should be ensured. Moreover, action in this area requires a balancing of various interests, as was confirmed by the Court of Justice in connection with the free movement of data. In this perspective, the majoritarian institutions may have a legitimate expectation that certain phenomena in society having a specific impact on the trustworthiness of governments are addressed by the DPAs, and that the DPAs take into consideration that various public interests need to be balanced. This expectation also implies not using resources in a disproportionate manner in dealing with claims of individuals, where the DPAs possibly are under an obligation to act.

A comparable dilemma—in relation to EU agencies—is characterised as a ‘Catch 22’ situation. On the one hand, the high degree of independence is the rationale for the role of DPAs. Precisely because of their independence they are considered as being an effective instrument for dealing with complex issues in a technological complex environment with big data and mass surveillance. On the other hand, there is the legitimate expectation that DPAs act in the wider interest of society, which requires that there must be some means to keep them under control.

Various tools could enhance the effectiveness of DPAs without prejudice to their independence. Examples are peer reviews, impact assessments or engaging with external experts. The use of these tools also enhances the accountability of DPAs.

---


1942 After the finalisation of the research it was reported that the case was withdrawn. However, in the near future similar questions may be raised before the Court of Justice.

1943 Case C-518/07, Commission v Germany, EU:C:2010:125, at 24.


1945 See, in relation to agencies, E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), 1395-1442.
13. **DPAs are Accountable to the Judiciary and Not Totally Free from Parliamentary Influence**

Accountability of DPAs as independent authorities means in the first place that they should be accountable for their acts before a court, under the rule of law. Article 74(1) of the proposed General Data Protection Regulation\(^{1946}\) states the obvious: “Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.”

In addition, in *Commission v Germany*\(^{1947}\) the Court of Justice of the European Union ruled that the independence of the data protection authorities does not free these authorities from any parliamentary influence by underlining that there should be some degree of parliamentary influence, illustrated by some examples. Albeit in an indirect manner, the Court thus underlined that DPAs are not only accountable for their acts before the judiciary under the rule of law, but that Member States must also ensure some degree of democratic accountability.\(^{1948}\)

In other words, the DPAs remain – to a certain extent – accountable towards the democratically elected institutions in society. The Court of Justice had already ruled on a similar matter in *Commission v European Central Bank*.\(^{1949}\) That ruling is even more precise than *Commission v Germany*. Independence of the ECB – which is, as was explained before, surrounded by strong safeguards – does not mean that the ECB is entirely separated from the EU framework and exempt from rules of EU law. The Court confirmed that there is judicial accountability before the Court itself as well as control by the Court of Auditors. Moreover, the ECB is subject to various other measures adopted by the EU legislature, such as, for instance, the data protection regime as laid down in Regulation 45/2001, including the control by the EDPS.

The ruling of the Court in *Commission v European Central Bank* can, therefore, be understood as meaning that the ECB operates within the institutional system of the European Union, and is accountable within this system. The same can be said about the DPAs under the Court’s case law.

The term accountability – as an obligation of public bodies, not to be confused with the accountability of data controllers and processors under EU data protection law\(^{1950}\) – is used in the literature both in a wider and a narrower sense.\(^{1951}\) In the wider sense it is similar to the notion of ‘good governance’; in a narrower sense it is described as the obligation to explain

---


\(^{1947}\) Case C-518/07, *Commission v Germany*, EU:C:2010:125, at 41-46, as explained in Section 9 above.

\(^{1948}\) Or, as Scholten calls it, political accountability, M. Scholten, The Political Accountability of EU Agencies: Learning from the US Experience (dissertation Maastricht, 2014).


and justify conduct. Here, the latter, narrow understanding is used, for the reason that we are focusing on accountability as a constraint for complete independence.

**Judicial accountability as compensation for the loss of full parliamentary control**

Under the rule of law, the procedures before the authorities and the possibilities for judicial review of the acts of the authorities must respect the rights to an effective remedy and fair trial. The requirement of a complete system of judicial protection follows from the right to an effective remedy and to a fair trial under Article 47 Charter.

This requirement plays a role in relation to the proposed General Data Protection Regulation. The issue is how effective remedies can be ensured in a multi-jurisdictional environment where DPAs of several Member States may be involved, and where judicial authorities of several Member States claim jurisdiction. In addition, where decisions are taken at the EU level that are of direct and individual concern to a person the Court of Justice has jurisdiction under Article 263 TFEU.

Full judicial accountability of expert bodies – and of DPAs in particular – can be seen as a means to compensate for the loss of democratic control. However, the expertise required for the governance of a technically complicated area may also inhibit full judicial control of the acts of these expert bodies. In this perspective, it makes sense to recall that the Court allows broad discretion in situations involving political, economic and social choices that require complex assessments and evaluations being made. In such cases, the Court exercises scrutiny in a restrained manner. The criterion “applied is not whether a measure adopted in such an area was the only or the best possible measure, since its legality can be affected only if the measure is manifestly inappropriate”.

Advocate General Cruz Villalón proposes transposing this approach to the activities of the ECB and expresses the view that judicial review must be cautious. One can question whether this same approach is appropriate in situations where powers are given to unelected bodies and where democratic control is by nature limited. Must the limitations in democratic

---

1952 Also in this narrower sense accountability is sometimes seen as more than judicial and democratic accountability, M. Busuioc & M. Groenleer in Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, at 192. We stick to judicial and democratic accountability, because this links directly to the rule of law and democracy, and closely links to legitimacy, as understood in this study (see Chapter 1, Section 2).


1954 The issue of giving decision making power to the European Data Protection Board led to intensive discussions in the legislative procedure, not at least because of its impact on Article 47 Charter.

1955 Case C-58/08, Vodafone and Others, EU:C:2010:321, at 52.

1956 Opinion AG Cruz Villalón in Case C-62/14, Gauweiler and others, EU:C:2015:7: “111. The ECB must accordingly be afforded a broad discretion for the purpose of framing and implementing the Union’s monetary policy. (58) The Courts, when reviewing the ECB’s activity, must therefore avoid the risk of supplanting the Bank, by venturing into a highly technical terrain in which it is necessary to have an expertise and experience which, according to the Treaties, devolves solely upon the ECB. Therefore, the intensity of judicial review of the ECB’s activity, its mandatory nature aside, must be characterised by a considerable degree of caution.”
control not be compensated by full judicial control? The answer to this question is not obvious.

Moreover, although different positions can be taken on the intensity of the judicial review in complex cases, it is beyond doubt that judicial accountability is an important element legitimising expert bodies such as DPAs. Judicial accountability of DPAs is wider than accountability before a judge in the exercise of its tasks. It also means that institutional aspects that apply to the DPAs as public authorities may be subject to judicial review.

The most obvious example is the removal from office of members of DPAs before their term has ended. According to the Court, the threat of a premature termination as such is incompatible with independence. Premature termination is, therefore, only possible under strictly limited conditions that relate to the person concerned and not to the performance of the tasks, and can only be pronounced by judicial authorities, or is at least subject to other strict rules and safeguards.

Other examples are staff rules or budget rules, which DPAs should comply with in the same way as any other public authority. They should also comply with rules on transparency. As far as these institutional aspects are concerned, compliance is not merely a legal obligation but it is also an expression of the democratic accountability of DPAs, or, in other words, their social responsiveness.

14. Democratic Accountability: Independence should Not mean that Expert Bodies act in a Non-Controllable and Arbitrary Manner

Independence should not lead to a situation in which expert bodies act in a non-controllable and arbitrary manner. In any event, there must be safeguards that these bodies act in a socially desirable way, in accordance with their mandate. This form of accountability should be ensured, also with a view to respecting the substance of the democratic structure of the state. However, the interpretation by the Court of Justice of the complete independence of DPAs seems to contradict the idea that these types of safeguards could be imposed. DPAs are independent in making policy choices, even if these choices may not always be socially desirable. This makes sense, in the light of the task of DPAs to protect a fundamental right that should not be dependent on the social perceptions of a majority and may even change.

1957 Case C-288/12, Commission v Hungary, EU:C:2014:237, e.g. at 54.
1961 As stated by M.Busuioc & M. Groenleer, EU Agencies in between Institutions and Member States, Edited by: Michelle Everson, Cosimo Monda, Ellen Vos, January 2014, at 175. See also Section 9.
1962 Critical reactions on the CJEU’s extensive interpretation of independence of DPA relate to the effects on the democratic structure, annotation to Case C-518/07, Commission v Germany, on the independence of data protection authorities by Jiří Zemánek 49 CMLR (2012), 1755–1768.
over time. The obvious example of a social perception that may be subject to change is the acceptance of the use of personal data for security purposes. In the period after a terrorist attack this acceptance may be different than before, but that does not mean that the independent body must adapt its position on how to ensure privacy and data protection. Of course, this is different where the changed social perceptions of a majority lead to a change of the law. The DPAs should respect the law.

The high standards for independence under EU law have as a consequence that an essential part of the enforcement of privacy and data protection is delivered by expert authorities outside the traditional trias politica, albeit under judicial control. This is even more relevant since their mandate focuses on privacy and data protection, but also requires that other interests need to be taken into account in decision-making processes.

Furthermore, although the national data protection authorities operate within the national jurisdiction, their actions may have cross-border effects and, in addition, they also have responsibilities at the EU level. This positioning further complicates the democratic legitimacy and accountability. It is not clear whether the DPAs are – primarily – accountable at the international level or the national level. The responsibilities of the DPAs at the level of the European Union will be even more predominant after the entry into force of the General Data Protection Regulation,1963 which intends to establish a mechanism of enforcement cooperation between the authorities and within a European Data Protection Board.

Whereas judicial accountability of DPAs for their performance is an obvious element of the functioning operation of these authorities under the rule of law, democratic accountability is a more complicated matter, since this aspect of accountability restricts the very nature of independence itself. In a slightly different wording: an essential element of the independence of DPAs is that their performance is not scrutinised by majoritarian bodies.1964

The wider context of accountability of public bodies: three perspectives

Bovens distinguishes three perspectives for considering accountability,1965 a democratic, a constitutional and a learning perspective. Although these perspectives are primarily relevant for elected bodies – accountability may have consequences in elections –, they also provide a good basis for scrutinising the accountability of DPAs.

The democratic perspective aims at giving the people control over activities of public bodies and goes back to the basics of a democracy. The position of a public body is the result of a chain of delegation and it is ultimately the people that transferred sovereignty to public

---

1964 This is the difference with agencies: DPAs do not have a principal to whom they are accountable. See on this in relation to agencies, M. Scholten, The Political Accountability of EU Agencies: Learning from the US Experience, (dissertation Maastricht, 2014), in particular Chapter 1.
bodies. Accountability in this perspective means that individuals are enabled to monitor and evaluate the performance of a public body. For DPAs this may mean that emphasis should be given to the transparency of their performance to the public. In this respect, a parallel exists with the obligations for the EU institutions to be transparent (Article 15 TFEU) and, under Article 11(2) TEU, to maintain an open, transparent and regular dialogue with representative associations and civil society.

The constitutional perspective relates to the control of government through checks and balances or institutional countervailing powers. The existence of DPAs in their role of supervising public authorities is justified, as such, because the DPAs are supposed to provide checks and balances, and where needed, to act as countervailing powers, to prevent the abuse of power by governments through the processing of personal information. However, as public authorities the DPAs should also act in an accountable manner. Mechanisms to ensure this are the judicial control of their performance, as well as the application of financial rules and control by a court of auditors.

The learning perspective of accountability is based on the idea that public bodies should be induced to learn. Accountability mechanisms should stimulate public bodies “to focus consistently on achieving desirable social outcomes”. In this context, for DPAs one could think of – publicly accountable – statutory requirements like peer reviews, impact assessments or engaging with external experts.

Another dimension of democratic accountability is the following. Democratic accountability is mainly implemented through ex post mechanisms, such as reporting obligations requiring authorities to explain their past performance and, more specifically, the consumption of the budget. However, there are also ex ante mechanisms. There is a connection. For instance, the budgetary procedures start with the process of the allotment of an annual budget to an authority and end with a discharge procedure, where the authority demonstrates how it has spent the allotted budget.

For DPAs, ex ante mechanisms are particularly difficult to reconcile with complete independence. In general, a DPA should not be obliged to justify to political institutions how it will exercise its tasks. This starting point is relevant, for instance, in relation to annual planning tools. It would be difficult to align with the independence of DPAs if they were required to submit an annual planning to parliament for a debate on priorities. However, a DPA does require a budget and in view of budgetary procedures it normally has to give a justification of the finances it intends to spend. This justification may, in practice, be even more important, to the extent that the Court of Justice in Commission v Austria did not

---

1967 These are just examples.
require the DPAs to have a separate budget line. In short, from the perspective of independence there are limits to the justifications that can be asked from a DPA in respect of its budget, but it is not fully clear what these limits entail.

Another instance where ex ante accountability plays a role is the selection procedure for the membership of DPAs. Scholten calls this, in relation to the appointment of EU top officials, including those heading EU agencies, a playground for political influence.\footnote{M. Scholten, The Political Accountability of EU Agencies: Learning from the US Experience, (dissertation Maastricht, 2014), at 77-90.} However, the selection procedure – provided it is executed in an appropriate manner – also legitimises the functioning of public bodies, including DPAs. As observed above,\footnote{See Section 10.} several guarantees could be included in a selection procedure in order to enhance the quality of the process, in terms of safeguarding ex ante accountability, ensuring that the procedure does not become a playground for political influence: involvement of different branches of government based on checks and balances, transparency of the process, and, last but not least, objective criteria for the selection.

**Instruments for democratic accountability: explaining and justifying conduct**

Parliamentary influence mentioned by the Court of Justice is not the only dimension of democratic accountability of DPAs. This can be illustrated by examples taken from Regulation 45/2001\footnote{Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.} – relating to the EDPS – and from the proposed General Data Protection Regulation.\footnote{Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.}

The most obvious example of accountability in the sense of explaining and justifying conduct is the obligation to submit an annual activity report\footnote{Also Article 28(5) of Directive 95/46 mentions the activity report, although it only should be submitted at “regular intervals”.} to the national parliament or the European Parliament – and to certain other public bodies – and at the same time to make it public.\footnote{Article 48 of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1 and Article 54 of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.} Regulation 45/2001 gives an interesting specification of the reporting obligation of the EDPS. The regulation mentions that supervised bodies – solely public bodies in the case of the EDPS – should be permitted to comment to the European Parliament on the follow up they have given to the remarks of the EDPS. Hence, the regulation introduces the submission of the annual report not only as an obligation on the EDPS to explain and justify its conduct, but also as an additional tool for the European Parliament to scrutinise the conduct of the EU institutions subject to supervision by the EDPS.
Other provisions relating to the DPAs do not have as their aim to ensure accountability in the sense of justifying and explaining conduct, but require transparency. The provisions on the procedures of appointment of members of DPAs – and their reappointment – are drafted in such a manner that they enhance accountability.\textsuperscript{1977} The DPAs as public bodies are subject to financial oversight. Practices of DPAs to perform their activities in a public manner and to publish their activities on the internet – although strictly speaking not required by EU law – have as an effect that they enhance the democratic accountability of DPAs in the narrow sense meant above.

\section*{15. Conclusions and a Model for Good Governance by DPAs}

The control on the data protection rules is mandated to the Union and within the Union to independent authorities. Article 8(3) Charter and Article 16(2) TFEU reflect that the system of control is a complete system: Compliance \textit{shall be} subject to the control of these independent authorities, operating with a high degree of independence as confirmed in the case law of the Court of Justice. DPAs derive their position from primary EU law, the control by the DPAs is a component of the fundamental right to data protection and under the case law of the Court the requirements for independence are high, excluding any direct or indirect external influence on the performance of their tasks.

An essential part of the enforcement of EU data protection law is assigned to expert bodies, which are primarily the DPAs of the Member States. These DPAs are independent public authorities that fulfil an important public task, but they are not accountable for their performance to the democratically elected bodies. The embedding of the role of DPAs in primary law gives them constitutional status. In the information society, their role is justified by the size of the issues at stake and by the fact that traditional methods are not sufficient. (Section 2)

The study identifies six reasons behind the existence of DPAs. First, historical reasons; second, the need for structural support in the area of data protection; third, the nature of data processing and the skills required for understanding data processing; fourth, the need for control of the private sector, but equally of governments themselves, when they process personal data; fifth, the need for independence from political preferences; sixth, the possibility to combine expertise and flexibility, and to dedicate their resources fully to data protection. (Section 3)

The DPAs have full competence under EU law, with a variety of roles. They are ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers. This does not mean that other bodies – like for instance national ombudsmen or agencies in neighbouring areas – cannot be competent in respect of certain matters concerning data protection, but their competence is not a derogation from the competence of the DPA. The variety of roles may

conflict with each other. As a policy advisor, the DPA may oppose a proposed legal instrument. However, after adoption of the instrument, the DPA must enforce the instrument. Another conflict may arise where DPAs cooperate with private entities, in developing frameworks for compliance, whereas they may be called upon to independently assess these frameworks in a later stage in the context of a complaint procedure. (Section 4)

A system with DPAs does not exist in the US. The most visible enforcement body is the Federal Trade Commission (FTC). FTC enforcement is described by several scholars as a big success factor of protection in the US, delivering ‘privacy on the ground’. Emphasis is given to the magnitude of financial penalties, as well as to forward-looking injunctions. FTC enforcement is also criticised. (Section 5)

The DPAs are a new branch of government: non-majoritarian expert bodies, which are in some respects different and in others similar to EU agencies. There are two main differences. First, EU agencies must respect general government policies, but the DPAs do not have to respect this type of guidance. Second, the requirements on what constitutes institutional independence are less strict for EU agencies. There are two main similarities. First, DPAs and EU agencies are both bodies composed of experts exercising public tasks and are in substance quite similar. Second, both operate in between the EU and the national levels. (Section 6)

DPAs qualify as new branches of government, in the theory of Vibert. DPAs do not derive their legitimacy from the other branches of government, as agents vis-à-vis a principal. By contrast, they should even be competent to supervise these other government branches within the traditional trias politica. This new branch of government could be instrumental in restoring trust, if the authorities operate within a context of checks and balances. The DPAs must act within the limits of their competence in accordance with the requirements of independence, effectiveness and accountability. Similar requirements have been developed for good governance of agencies. (Section 7)

EU agencies and DPAs are expert bodies in between the EU and national levels. EU agencies are EU bodies established under EU law, but, in return for agreeing to their establishment, the Member States have ensured that national influence is retained. DPAs are national bodies established under national law, but once established, they exercise tasks attributed to them by primary EU law. There is a tendency to give national interests a stronger say in the functioning of EU agencies, but the national autonomy in relation to DPAs has diminished and this will be even clearer under the General Data Protection Regulation. (Section 8)

Under the case law of the Court of Justice, complete independence of DPAs means that no external influence is allowed. Independence is supposed to make supervision more reliable. Reliability of supervision is an objective, because the supervision affects the social sphere of individuals. Independent, reliable supervision contributes to its legitimacy. The high standard for independence of DPAs also includes an organisational distance to the executive. Their task includes the balancing of various interests – with a broader scope than the rights to privacy and data protection – which, according to the Court, requires distance from majoritarian policy-making to ensure a fair decision-making process. Still, there should be
some degree of accountability towards political institutions, especially to parliaments and the judiciary. (Section 9)

The complete independence of DPAs confirms their status as a new branch of government. This independence differs from the autonomy of EU agencies, which is an autonomy from the influence of market forces, but not from political majorities. The appointment of members of DPAs is a critical factor potentially influencing independence. This study suggests involving the legislative, the executive and the judiciary branch in the appointment procedure, to ensure checks and balances and to avoid that political preferences play a decisive role in the appointment. Also the DPAs themselves have an obligation to safeguard their own independence, vis-à-vis the other branches of government and the private sector. (Section 10)

The effectiveness of DPAs is subject of debate. There is a presumed lack of effectiveness and the DPAs struggle for resources. Also the Fundamental Rights Agency of the European Union reported on a great variation as well as on deficiencies in the powers and the resources of the DPAs: it reported on understaffing and a lack of adequate financial resources of DPAs, with the result that in many Member States the DPAs do not carry out all their tasks. As a rule, sanctioning powers are restricted in view of the fact that the DPAs should be able to effectively enforce infringements, although the sanctioning powers are gradually changing. This is addressed in the General Data Protection Regulation, but in the meantime it is an obligation for the Member States to ensure effectiveness. After the entry into force of the General Data Protection Regulation, this obligation remains with the Member States, but will be subject to precise parameters set by EU law. (Section 11)

DPAs should have effective powers, particularly in the developing information society. Member States should guarantee protection by DPAs, in accordance with the principles of equivalence and effectiveness. Proximity, meaning that an individual is entitled to protection by a DPA in his own Member State, is not required under EU law, but could enhance the effectiveness of protection since it counterbalances forum shopping by big internet companies, choosing a Member State of establishment on the basis of the (lack of) enforcement capacity of its DPA. DPAs are free to set their own agenda, but with one limitation, which is their obligation to handle complaints. That is exactly the obligation that is the subject of the pending case Rease and Wullems. (Section 12)

Accountability of DPAs as independent authorities means in the first place that they are accountable for their acts, before a court, under the rule of law. As the General Data Protection Regulation confirms, everyone has the right to a judicial remedy against decisions of a DPA concerning him or her. In addition, the independence of the data protection authorities does not free these authorities from any parliamentary influence, although this influence is by definition limited. Judicial accountability is a compensation for the loss of full parliamentary control. (Section 13)

Expert bodies should not act in a non-controllable and arbitrary manner. The fact that national DPAs, on the one hand, are part of the national administration, and, on the other
hand, act as agents of the European Union further complicates the democratic legitimacy, and also the judicial accountability. It is not clear whether the DPAs are – primarily – accountable at the national level or at the EU level. The study distinguishes three perspectives based on the work of Bovens. Under the democratic perspective, the DPAs should ensure transparency of their performance to the public. Under the constitutional perspective, checks and balances for DPAs should be judicial control, the application of financial rules and control by a court of auditors. Under the learning perspective DPAs should profit from peer reviews, impact assessments or engaging with external experts. (Section 14)

A model for good governance for data protection authorities is proposed, as a specific tool for further improving the level of protection. This model is inspired by the LITER Good Agency Principles,\textsuperscript{1978} which aim at making agencies work better, and should include the following elements:

- DPAs should in the course of all their actions protect their own independence and ensure that they do not take any external instruction.
- DPAs should effectively operate in between the EU level and the Member States, emphasising ‘proximity’ to the individual in their working methods.
- DPAs should demonstrate the results of past performance (accountability \textit{ex post}), by reporting in a public manner, and allowing public debate. This obligation should be exercised without prejudice to the complete independence they enjoy vis-à-vis elected bodies.
- Transparency is a factor determining accountability during the process. Transparent working methods – such as peer reviews and impact assessments – could be instrumental in this perspective.
- Guarantees must be included in appointment procedures, involving various branches of government.
- The principle of sincere cooperation determines the cooperation of DPAs with EU bodies, but also with each other. DPAs should invest in cooperation in extraterritorial investigations.
- Under the principle of sincere cooperation, the DPAs are also encouraged to cooperate with EU agencies and national regulatory authorities with competences in other policy areas.
- Cooperation with the private sector is encouraged, but subject to the condition that responsibilities are not blurred.
- As public authorities DPAs should ensure that they include other public interests in their decision-making. Besides basing their assessment on the legal provisions on data protection, they should also take account of the wider context.
- Data protection law (for example Directive 95/46) assumes that DPAs also have advisory tasks, which may conflict with their role as supervisor as envisaged by the Treaties. This conflict raises two issues:

- It must be ensured that DPAs supervise legislation in an objective manner, even after having criticised this legislation in the legislative process.
- In ‘accountability’ schemes, the supervisor must not become co-responsible for solutions at an individual level.

- Implementing and Delegated acts (Articles 290 and 291 TFEU) should not be used as instruments by the Commission to make DPAs comply with changing views in society. Giving guidance to DPAs should be a task solely for the Article 29 Working Party, the institutionalised network of DPAs.
Chapter 8. Understanding the Role of Cooperation Mechanisms of DPAs: Towards a Layered Model of Horizontal Cooperation between DPAs, a Structured Network of DPAs and a European DPA

1. Introduction

The Data Protection Authorities (“DPAs”) should also ensure compliance with data protection rules where the data controller, the processor or the personal data (cloud computing) are located outside their jurisdiction, and where the DPAs do not have effective jurisdiction and enforcement powers. This requires cooperation with other DPAs. Control by DPAs is an essential element of data protection and cooperation between DPAs is an essential element of the control.

This chapter analyses the contribution of the cooperation mechanisms of DPAs to the EU mandate under Article 16 TFEU. This analysis is a specification of an element of the research question: “what does and should the European Union do to make Article 16 TFEU work, through the cooperation of independent authorities?” This analysis includes the following subjects:

a. the general design of the cooperation of DPAs;
b. the state of play of the cooperation under current law and the role of the Article 29 Working Party;
c. the novelties to be introduced by the General Data Protection Regulation: the one-stop shop and consistency;
d. the experience in the area of electronic communications and cooperation in the context of developing EU administrative law;
e. three models: horizontal cooperation, a structured network and a European DPA;
f. ensuring independence, effectiveness and accountability in the cooperation of DPAs.

The first objective of the chapter is to assess the cooperation mechanisms of DPAs, as part of a composite EU administration, against the background of developing EU administrative law. The second objective is to introduce three models of cooperation, against the background of the proposed General Data Protection Regulation (“GDPR”). The cooperation with authorities in third countries will be discussed in Chapter 9.

Section 2 presents cooperation as an instrument for DPAs to protect individuals in a cross-border context and to contribute to a harmonised and effective level of data protection within the wider territory of the Union. Therefore, DPAs’ mandate has an EU-wide component: their

1979 As explained in Chapter 7, with reference to Case C-518/07, Commission v Germany, EU:C:2010:125, at 23.
1980 See Chapter 7, Section 1.
task is not solely to protect persons residing in their own Member States, but also individuals all over the Union, or more precisely, to contribute to the protection of these individuals. This part of their mandate further illustrates that the DPAs operate in between the Member States and the Union.

Sections 3 and 4 of this chapter explain the state of play in the European Union, in relation to the exercise of the tasks of DPAs in a cross-border context and in particular their mutual cooperation and institutional mechanisms for such cooperation. Section 5 discusses two main novelties introduced by the proposed General Data Protection Regulation. These are a one-stop shop mechanism, with a lead supervisory authority, and a consistency mechanism, with a central role for the European Data Protection Board ("EDPB"), that must be set up under the regulation.

Sections 6 and 7 show the wider context of the multi-jurisdictional aspects of control by DPAs. They refer to experiences in the related area of electronic communications and to theories on cooperation between authorities in different jurisdictions. The perspective chosen is administrative law, since many of the issues arising in relation to the operation of DPAs and their mutual cooperation have parallels with the wider discussions on EU administrative law and with the debate on the need for harmonised rules on procedural law in the European Union.1981

The various models for cooperation are the subject of Sections 8 to 11. These models are the horizontal cooperation between DPAs, a structured network of DPAs and the cooperation within a European DPA. Variations between these models may also exist, as illustrated by the EDPB, which will have elements of both a structured network and a European DPA. Section 12 contains an analysis from the perspectives of independence, effectiveness and accountability. Section 13 contains conclusions.

A final remark relates to the main substance of this chapter. It is dedicated to control of EU law by public authorities and does not deal with the involvement of private parties in the control. As was explained in Chapter 6, the governance with involvement of private parties plays an important role in privacy and data protection, in particular on the internet, but it exceeds the scope of this chapter, which does not concern multi-level governance in this wider sense.1982

2. A General Design of DPAs Cooperating with Each Other and in Composite Administrations or Trans-Governmental Networks

---


Article 16(2) TFEU and Article 8(3) Charter attribute the task of ensuring control of the protection of the fundamental rights of privacy and data protection to the DPAs. The task of the DPAs comprises the obligation to contribute to a harmonised and effective level of data protection within the wider territory of Union. This is particularly important in an internet environment, where dealing with cross-border effects is an inherent element of the protection that must be given. Moreover, this obligation for DPAs is the consequence of the recognition that the European Union is the appropriate platform for dealing with internet privacy and data protection. Article 46(1) of the Proposal for a General Data Protection Regulation makes this obligation explicit.\(^\text{1983}\) The obligation also exists – although in a more implicit manner – under current data protection law.\(^\text{1984}\)

Hence, the mandate of the DPAs has an EU-wide component. This component of the mandate does not fully fit in our understanding of the division of competences between the Member States and the Union. The DPAs are hybrid in character, operating in between the Member States and the Union. Whereas, as a rule, the competences are divided between the European Union and the Member States,\(^\text{1985}\) the cooperation mechanisms between DPAs are an example of competences that are not divided, but shared.\(^\text{1986}\)

Cooperation has an impact on the independence of the DPAs, for instance because national DPAs should mutually cooperate with their peers in other Member States and take the positions of these peers into account. Cooperation is a requirement for effective protection, but may also adversely affect the effectiveness of the exercise of the tasks of the DPAs. For instance, where DPAs must dedicate resources to ensure data protection outside their national jurisdictions, this will limit the resources available for purely national protection.

In addition, judicial accountability must be guaranteed through the existence of judicial review mechanisms in a multi-level legal environment. The democratic accountability – which is not evident for these expert bodies, as was explained in Chapter 7 – becomes even more complicated where DPAs operate at multiple levels, in European networks.\(^\text{1987}\)

This chapter analyses how the cooperation is carried out and how the institutional mechanisms function, from the perspectives of independence, effectiveness and democratic as well as judicial accountability. The chapter examines the obligation of DPAs to contribute to data protection in the whole of the European Union as an additional component of their mandate to ensure control over the protection of the fundamental rights to privacy and data.

---

\(^\text{1983}\) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.

\(^\text{1984}\) Recital 65 and Articles 29 and Article 30 (1) (a) of Directive 95/46.

\(^\text{1985}\) As explained in Chapter 4. Even the domain of shared competence, as specified in Article 2 (2) TFEU essentially means a procedure for the division of competences.


protection under EU law. This component also includes the obligation of the DPAs to cooperate with one another, an obligation that serves “to ensure that the rules of protection are properly respected throughout the Union”.\textsuperscript{1988} Cooperation of DPAs is also a means to forego forum shopping by regulatees in an attempt to engage the authority that is perceived as most convenient.\textsuperscript{1989}

The chapter builds on Chapter 7, which already highlighted the hybrid nature of the DPAs. As a rule – the European Data Protection Supervisor is the exception – the DPAs operate in between the European Union and the Member States. The DPAs are authorities established within the national legal order, but who act as agents of the European Union, with a mandate to ensure control of the EU rules on privacy and data protection within the national jurisdictions. This chapter demonstrates that the hybrid nature also includes a responsibility outside the jurisdiction in which the DPAs are established. The DPAs cooperate in what is defined as “multi-jurisdictional networks”\textsuperscript{1990} or as a European composite administration.\textsuperscript{1991}

The obligation of DPAs to cooperate also has institutional aspects. Under EU law, various mechanisms for institutional cooperation between the DPAs have been established, with the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the “Article 29 Working Party”) as the most prominent example. The General Data Protection Regulation intends to strengthen the institutional cooperation within the framework of the EDPB, which still must be set up. These institutional mechanisms for cooperation are further actors in ensuring the respect of privacy and data protection under EU law. These institutional mechanisms are not provided for in the Treaties. Hence, their tasks are not attributed by primary EU law, but derived from the tasks of the DPAs. This means, as a basic condition, that where these mechanisms have a role in ensuring control on the rules on data protection, this should not compromise the independence of the DPAs.

Cross-border cooperation is particularly important in view of the challenges resulting from the developments in the information society.\textsuperscript{1992} In an information society, the processing of personal data is in many situations not confined to one jurisdiction and has an inherent cross-border effect. Cross-border cooperation of supervisory authorities is a conditio sine qua non for effective control. Directive 95/46 on data protection acknowledges this, for instance where it includes an obligation for DPAs to exchange all useful information.\textsuperscript{1993} However, the effectiveness of enforcement cooperation and of harmonised approaches in enforcement is not self-evident. The need to improve consistency in the enforcement of data protection rules across Europe was an important trigger for the Commission to initiate the data protection

\textsuperscript{1988} Recital 64 of Directive 95/46.
\textsuperscript{1989} See on this, E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), pp. 1395–1442, at 1412.
\textsuperscript{1991} Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57.
\textsuperscript{1992} As explained in Chapter 3.
\textsuperscript{1993} Article 28(6) of Directive 95/46.
reform. One of the objectives of this reform is to avoid inconsistent responses of EU data protection authorities to services offered on the internet.\textsuperscript{1994}

This chapter analyses the judicial and democratic accountability of DPAs with a different focus from that used in Chapter 7. Whereas Chapter 7 emphasised the accountability of DPAs as unelected bodies, the present chapter deals with aspects of judicial and democratic accountability as a consequence of the fact that the DPAs operate in multiple jurisdictions.

**DPAs operating in multiple jurisdictions: a challenge to reconcile independence, effectiveness and accountability, as illustrated by the GDPR**

DPAs are national authorities that fulfil a role under EU law. This has a positive impact on the legitimacy of EU action in the area of privacy and data protection. Their role is comparable to the roles of national and EU agencies operating in between the national and the Union level.\textsuperscript{1995} These roles include both contributing to harmonisation within the European Union and safeguarding national specificities.

However, the fact that DPAs operate in multiple jurisdictions may adversely affect their democratic legitimacy and accountability. As was explained in Chapter 7, in *Commission v Germany*,\textsuperscript{1996} the Court of Justice of the European Union ruled that the independence of DPAs does not free them from every parliamentary influence. The question arises which parliament is entitled to exercise influence, because DPAs operate in composite administrations\textsuperscript{1997} or transgovernmental networks.\textsuperscript{1998} The DPAs are not only separated from the democratic structure within the jurisdiction in which they operate, but they are also separated from the specific jurisdiction itself, since they operate on various jurisdictional levels.\textsuperscript{1999}

This situation also affects the judicial accountability. Where DPAs operate in multiple jurisdictions, in particular in an institutional setting, multiple actors in multiple jurisdictions may bear legal responsibility for the same act. Bignami argues that under current EU data protection law the judicial accountability – expressed in terms of standards of judicial review – is not affected by the involvement of multiple jurisdictions, in any event not in a similar


\textsuperscript{1995} As explained in Chapter 7, Section 8.


\textsuperscript{1997} Term used by Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57.


\textsuperscript{1999} In the words of Lind and Reichel, they are cut loose from their foundation in the national and the European legal order, Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57, at 53-54.
way as the democratic or political accountability. However, an appropriate standard of judicial review will not necessarily be guaranteed under the General Data Protection Regulation.

Independence, effectiveness and judicial and democratic accountability should be reconciled in a satisfactory way. The extensive discussions in the Council on the one-stop shop mechanism and the consistency mechanism illustrate that this result is not easy to reach. The one-stop shop mechanism and the consistency mechanism were proposed with the objective of increasing the effectiveness of data protection within the European Union. In all cases, the enforcement of EU data protection law should result in a single decision with EU-wide application.

This objective of increasing effectiveness did not convince everyone. It was stated that these mechanisms are not achieving a better protection for the data subjects and that it is mainly the businesses who benefit (in their capacities as data controllers or data processors).

However, individuals may feel that decisions are taken at a considerable distance, and the rights to an effective remedy and fair trial as laid down in Article 47 Charter may not be sufficiently respected. The mechanisms may result in a situation where an individual no longer has effective redress before the DPA in the Member State where he or she resides. The term ‘proximity’ was used as a requirement for legitimate and accountable protection.

Moreover, as this chapter explains, the current mechanisms are already complicated and with the introduction of further mechanisms under the General Data Protection Regulation the complexity increases, possibly leading to legal uncertainty. These (new) mechanisms put the legitimacy of the protection at risk.

3. Cross-Border Enforcement and Mutual Cooperation between DPAs: The State of Play

The EU-wide component of control by national DPAs and the task of the Member States to secure the effectiveness and uniformity of EU law

As was explained, the control by DPAs is an essential component of the right to data protection itself. However, primary EU law is silent on the exercise of the tasks of DPAs in a cross-border context and on their mutual cooperation, whether or not in the context of


2001 See Section 12.

2002 Council of the European Union, various Council documents on Council Public Register, re Interinstitutional file 2012/0011 (COD), e.g. 18031/13 (19 Dec 2013, full version on lobbyplag.eu) and 14788/1/14 (13-11-2014).

2003 Council of the European Union, various Council documents on Council Public Register, re Interinstitutional file 2012/0011 (COD), e.g. 18031/13 (19 Dec 2013, full version on lobbyplag.eu).


2005 See Chapter 7, Sections 1 and 2.
institutional mechanisms. Article 16(2) TFEU and Article 8(3) Charter provide that the DPAs shall ensure control, not how they shall do this.

The duty for ensuring control in a cross-border context and for mutual cooperation follows directly from the system of EU law. There is a parallel with the remedies that must be provided under national law to ensure the legal protection against breaches of provisions of EU law. Dougan defines this as securing the effectiveness and uniformity of EU law, based on the requirements of equivalence and effectiveness, established by the European Court of Justice in *Rewe-Zentralfinanz* Enforcement cooperation between DPAs is a specification of the principle of sincere cooperation under Article 4(3) TEU that obliges all national authorities to remedy breaches of EU law. To put it simply, on the internet the DPAs must remedy breaches of EU data protection law in an effective manner that necessarily comprises DPA cooperation in cross-border situations. Cooperation between DPAs is also a tool to ensure the uniformity of EU law.

*The state of play in data protection law*

Various provisions of Directive 95/46 on data protection specify the general requirements under EU law for cross-border enforcement and mutual cooperation, albeit not in a very precise manner. Recital (64) of the directive declares that the DPAs must assist one another in performing their duties. A DPA may be requested to exercise its powers by a DPA of another Member State; the DPAs cooperate “to the extent necessary for the performance of their duties, in particular by exchanging all useful information”. The purpose of this all is “to ensure that the rules of protection are properly respected throughout the European Union”. The Article 29 Working Party mentions as a further purpose bridging the gap between applicable law and supervisory jurisdiction.

Council of Europe Convention 108 is more explicit and contains a framework for mutual assistance between the member states of the Council of Europe, which are parties to the Convention, and the authorities within these states. This framework for assistance

---

2010 Article 28(6) of Directive 95/46.
2011 Recital (64) of Directive 95/46.
2013 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.
2014 Chapter IV of the Convention, as described by Dariusz Kloza and Anna Moscibroda, Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law, International Data Privacy Law, 2014, Vol. 4, No. 2, at 121-122.
provides for instance that assistance must be given to data subjects residing abroad.\textsuperscript{2015} Under the Additional Protocol to the Convention,\textsuperscript{2016} the DPAs must ensure “that people are able to exercise their rights on an international as well as a national level”.\textsuperscript{2017}

The proposed General Data Protection Regulation\textsuperscript{2018} is even more specific on cross-border enforcement and mutual cooperation. Although this chapter focuses on the current state of EU law, many examples originate from this proposal, for a simple reason: the proposal elucidates the main issues at stake. The proposal distinguishes – under the heading of “cooperation”\textsuperscript{2019} – between cross-border enforcement and mutual cooperation. Equally, the proposal deals – under the heading of “consistency”\textsuperscript{2020} – with the institutional cooperation between the DPAs.

\textit{Three types of enforcement cooperation of DPAs}

This section distinguishes three types of enforcement cooperation of DPAs. These types vary as far as the impact on the task of the DPAs is concerned.\textsuperscript{2021}

The first type of cooperation is the exchange of information between DPAs, which is explicitly mentioned in Article 28(6) of Directive 95/46 as an obligation for DPAs. The exchange of information is – in a general sense – the essence of the procedural cooperation between authorities.\textsuperscript{2022} The exchange may consist in the establishment, generation and sharing of information needed for decision-making.\textsuperscript{2023} The exchange of information on individuals was the subject matter of \textit{Commission v Spain},\textsuperscript{2024} relating to the Schengen Information System. The Court of Justice ruled that the obligation of providing information to an authority in another Member State as a basis for decision-making by the latter may not be satisfied by inserting an alert on an individual in the system as was explicitly required by law, but that – under certain circumstances – supplementary information must be provided.\textsuperscript{2025} \textit{Commission v Spain} illustrates that the obligation is not fulfilled by merely implementing specific provisions of EU law, but that fulfilling the obligation requires an

\textsuperscript{2015} Article 14 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108
\textsuperscript{2016} Article 1 (5) of Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.
\textsuperscript{2017} Explanatory Report on Article 1 (5) of the Additional Protocol.
\textsuperscript{2021} This distinction is largely in line with Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure: Introduction to the ReNEUAL Model Rules Book V - Mutual Assistance, (at 205). However, this chapter does not include “service of documents” which does not seem relevant for data protection, whereas it does include the joint investigations, which are not part of the ReNEUAL Model Rules.
\textsuperscript{2024} Case C-503/03, Commission v Spain, EU:C:2006:74.
\textsuperscript{2025} Case C-503/03, Commission v Spain, EU:C:2006:74, at 56.
active approach in assisting authorities in other Member States, where this is reasonably expected.

A second type of cooperation consists in effectively assisting in supervision, such as carrying out inspections at the request of a DPA in another Member State.\textsuperscript{2026} This cooperation takes place on a regular basis, for instance where a complaint lodged by an individual in a Member State concerns a data controller established in another Member State, where evidence needs to be gathered in the jurisdiction of another Member State, or where a controller is established in several Member States.\textsuperscript{2027}

An example is the cooperation between DPAs in enforcement actions against internet companies. Kloza & Moscibroda\textsuperscript{2028} describe the examination of Google's privacy policy in 2002-2013 by several DPAs, working together in an informal task force initiated by the Article 29 Working Party. The initial investigations by this task force were followed by further investigations by the participating DPAs, resulting in separate decisions.

Neither Directive 95/46 nor any other instrument of EU data protection law provide a clear legal basis for this type of cooperation. However, this does not imply that this type of cooperation purely takes place on an informal basis or based on bilateral arrangements between Member States. An obligation to cooperate can be deduced from Article 28(6) of Directive 95/46, read in combination with recital (64) thereof, which emphasise the need for Member States and for DPAs to assist one another. Furthermore, under the principle of sincere cooperation\textsuperscript{2029} the DPAs are required to cooperate with each other in enforcement actions.

Article 56 of the Proposal for a General Data Protection Regulation\textsuperscript{2030} introduces a third type of enforcement cooperation. This type consists of the carrying out of joint investigative tasks, joint enforcement measures and other joint operations. This is a further step towards empowering DPAs to ensure the control of EU data protection law where individuals are affected by acts relating to the processing of personal data outside the jurisdiction where they have their usual residence. This type of cooperation is not regulated under present EU law, although it is reported that DPAs have experiences with joint investigations.\textsuperscript{2031}

\textbf{4. Institutional Arrangements: Article 29 Working Party and Other Mechanisms for Institutional Cooperation between DPAs}

\textsuperscript{2026} Example taken from Article 55(1) of Commission Proposal for a GDPR, COM (2012), 11 final.
\textsuperscript{2027} Article 29 Data Protection Working Party, Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC, 20 April 2011, at Addenda.
\textsuperscript{2029} Article 4(3) TEU.
\textsuperscript{2030} Article 56 of Commission Proposal for a GDPR, COM (2012), 11 final.
\textsuperscript{2031} Article 29 Data Protection Working Party, Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC, 20 April 2011, at 1.
Under present EU law, several mechanisms for institutional cooperation of DPAs have been set up. The core mechanism is the Article 29 Working Party, which operates in a broad area of privacy and data protection. Other mechanisms have been set up for restricted areas within EU data protection, in particular in the area of freedom, security and justice (Title V of the TFEU).

Within the mandates of these mechanisms for institutional cooperation a distinction can be made between advisory and supervisory roles, or to remain closer to the terminology of Article 16(2) TFEU and Article 8 Charter: giving advice and guidance on how to ensure control on the one hand and effectively ensuring control on the other hand.

The Article 29 Working Party is an advisory mechanism, set up under Article 29(1) of Directive 95/46 on data protection. The Article 29 Working Party is composed of representatives of national DPAs and of the European Data Protection Supervisor. The European Commission is also a member, albeit without voting rights.2032

The Article 29 Working Party is a body that establishes a connection between tasks of the national DPAs and tasks of the Commission,2033 in particular by contributing to the uniform application of the national rules adopted pursuant to Directive 95/46.2034 The task of contributing to the uniform application is directly connected to the task of the DPAs to monitor the application of Directive 95/46,2035 which, as was explained above, implies contributing to the consistent application of EU data protection law. This task is made explicit in the General Data Protection Regulation.2036 The task is also directly connected to the role of the Commission as guardian of the Treaty, in which capacity it is committed to EU integration.2037

The Article 29 Working Party focuses on coordination, planning and guidance through soft law instruments and has no powers to intervene in individual cases. As a result, data protection is not applied in a fully harmonised manner in the Member States. The differences between the enforcement practices in the Member States were an underlying reason for the Commission to propose the reform of the EU data protection law.2038 Jóri gives an illustrative example based on his experience as head of a DPA in Hungary, where he argues that differences between Member States relate to the advisory role of the DPAs, and that, where this advisory role – he calls this the role of privacy advocate – is less developed, the independence of the DPAs is at risk.2039

2032This follows from Article 29(2) and (3) of Directive 95/46.
2034 Recital 65 and Article 30 (1) (a) of Directive 95/46, as explained in Section 3.
2035 Article 28(1) of Directive 95/46.
2036 Article 46(1) of Commission Proposal for a GDPR, COM (2012), 11 final. See also Section 2 above.
2038 As was explained above in Chapter 7, Section 11.
In short, a core task of the Working Party is to contribute to the uniform application of the national rules adopted pursuant to Directive 95/46. The further task of contributing to a harmonised and effective level of data protection within the wider territory of the European Union is also mainly attributed to the Working Party. The contribution of the Working Party consists of non-binding, soft law instruments aimed at harmonisation in a non-coercive way.

Although the Article 29 Working Party does not have a formalised role in supervision of data protection, it indirectly influences the supervision by the DPAs in a significant manner, because it gives guidance for enforcement. This guidance is in some occasions quite precise, as is illustrated by the guidelines of the Working Party for the implementation of the ruling of the Court of Justice in Google Spain and Google. These guidelines indicate in a precise manner what is expected from search engines and “they contain the common criteria to be used by data protection authorities when addressing complaints”. By using this formula the Article 29 Working Party does not seem to be limiting itself to a strictly advisory role. Another example is the involvement in the enforcement measures in respect of Google’s privacy policy, where the Article 29 Working Party played an initiating role, which resulted in enforcement actions of a number of national DPAs, including the French CNIL.

Under the General Data Protection Regulation, the institutional mechanisms for cooperation will be reinforced by a consistency mechanism, which includes an explicit role in enforcement. Moreover, Article 52(1)(j) of the Commission proposal provides for a duty for the DPAs to participate in the activities of the EDPB, the successor of the Article 29 Working Party. This duty does not exist under current law.

Other mechanisms for institutional cooperation, mainly in the area of freedom, security and justice

The Joint Supervisory Bodies, established for the supervision of respectively Europol and Eurojust, are institutional mechanisms with the aim of effectively ensuring control on the

---

2040 Recital 65 and Article 30 (1) (a) of Directive 95/46.
2041 Terminology taken from E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), pp. 1395–1442, at 1409.
2042 Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” - WP 225.
2043 Letter from the Article 29 Working Party to Google on the right to be delisted, 6 January 2015. Similar letters were sent to other providers of search engines. See also the Press Release of 18 June 2015 of the Article 29 Data Protection Working Party on Delisting, explaining the functioning of the guidelines.
2044 As referred to in the previous section and explained by Dariusz Kloza and Anna Moscibroda, Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law, International Data Privacy Law, 2014, Vol. 4, No. 2, at 125-127.
processing of personal data by these two EU agencies, which are active in the area of police and judicial cooperation in criminal matters. The Joint Supervisory Bodies are composed of representatives of national DPAs, with guarantees for the independence of their members, and are responsible for the supervision of data protection in relation to the two EU agencies. The core task of both Europol and Eurojust is to analyse information that to a large extent originates from the national police and the national judiciary. The benefits of this tailor-made regime were underlined by Alonso Blas. However, the functioning of the Joint Supervisory Bodies is also criticised, because the bodies do not comply with the requirement of independence of DPAs set by the Court of Justice and because of their apparent lack of effectiveness. This criticism is not further analysed here. This section only recalls that these bodies are mechanisms for institutional cooperation between national DPAs that aim at ensuring effective enforcement by involving national DPAs in the supervision of an EU agency.

The mechanism of coordinated supervision included in several instruments in the area of external border control, asylum and immigration is a hybrid mechanism with advisory and supervisory components. This mechanism currently exists for the Schengen Information System, the Visa Information System (VIS) and Eurodac. In another area of EU

---


2048 To be complete, a Joint Supervisory Authority also exists for a part of the Customs Information System. Since data protection supervision of the Customs Information System has a complicate structure (resulting from the former pillar structure of the EU Treaties) and has limited practical relevance, it is only mentioned in footnotes.


2053 To be complete, this mechanism also exists for a part of the Customs Information System (the part not covered by the Joint Supervisory Authority).


2056 Article 32 of Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No
law, this mechanism was set up for the Internal Market Information System.\textsuperscript{2057} All these information systems are composed of national parts, under the supervision of national data protection authorities, and of a European part supervised by the European Data Protection Supervisor (EDPS). Coordinated supervision refers to the coordination between the national supervisory authorities and the EDPS and consists for instance of the exchange of relevant information, assisting each other in carrying out audits and inspections, and examining difficulties of interpretation or application of the law.\textsuperscript{2058} In this mechanism, the national DPAs and the EDPS cooperate in a non-hierarchical manner.\textsuperscript{2059}

\textit{The European Data Protection Supervisor}

The European Data Protection Supervisor (EDPS) is not a mechanism for institutional cooperation of DPAs. The EDPS is the independent authority ensuring the control on the compliance with data protection rules at the level of the European Union itself. The Members of this authority – the Supervisor and the Assistant Supervisor – are appointed by common accord of the European Parliament and the Council, on the basis of a list drawn up by the Commission.\textsuperscript{2060} Neither the appointment procedure, nor the management structure has any direct link with the national DPAs.

However, the EDPS has the general duty to cooperate with the national data protection authorities.\textsuperscript{2061} He takes part in the institutional cooperation mechanisms, in principle on an equal footing with the other DPAs. His participation in the Article 29 Working Party is mandatory.\textsuperscript{2062} The Rules of Procedure of the EDPS specify this role. They underline the active contributions of the EDPS to the common interpretation of provisions of EU data protection law and specify that the EDPS shall put forward the Union perspective, where appropriate.\textsuperscript{2063} The EDPS, acting in accordance with this commitment, should reinforce the quality of the work of the Article 29 Working Party and, by doing so, enhance the accountability and effectiveness of the Working Party. This makes the EDPS an additional

\textsuperscript{2058} As specified in the legal bases quoted in the previous footnotes.
\textsuperscript{2059} See on the non-hierarchical cooperation Anna-Sara Lind and Jane Reichel, Administering Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57, at 47 and discussed below in Section 9.
\textsuperscript{2060} Article 42(1) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
\textsuperscript{2061} Article 46(f)(i) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
\textsuperscript{2062} Article 46(g) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
safeguard for a legitimate and effective control of the compliance with data protection rules, also in the Member States.

5. Two Main Novelties in the Proposed GDPR: A One-Stop Shop Mechanism and a Consistency Mechanism

A one-stop shop mechanism with a lead supervisory authority cooperating with its peers

The Commission Proposal for the General Data Protection Regulation provides for a one-stop shop,\textsuperscript{2064} Where the processing of personal data takes place in more than one Member State, one single DPA should be competent for the enforcement, for the following reasons: to increase the consistency in the application of the data protection rules, to provide legal certainty and to reduce the administrative burden for the controllers and processors of personal data.\textsuperscript{2065} This proposal has been transformed by the European Parliament\textsuperscript{2066} and the Council\textsuperscript{2067} into a mechanism where this single DPA acts as a lead supervisory authority, acting in close cooperation with other concerned authorities. The Council specifies in detail the competences of the lead authority and how the cooperation of the lead authority with other DPAs should be conducted.

The elaborations by the European Parliament and the Council prevent the single DPA from acting without considering the views of other DPAs involved and also respond to the criticism that the one-stop shop would lead to an exclusive competence of one DPA and not to a structured system of cooperation between DPAs.\textsuperscript{2068}

The structured cooperation mechanism now included in the legislative documents of the Council and the European Parliament allows other concerned DPAs to raise objections, but, at the end of the day, all DPAs concerned are bound by the decision of the lead DPA.\textsuperscript{2069} This is a novelty compared to the current regime under Directive 95/46, where the same data processing operation may be subject to diverging enforcement actions initiated by DPAs in various Member States.\textsuperscript{2070} As an illustration, in 2015 the Belgian DPA carried out an investigation in relation to the allegation that Facebook did not only process the personal data

\textsuperscript{2064} Recital (98) of Commission Proposal for a GDPR, COM (2012), 11 final.
\textsuperscript{2065} Recital 97 of the proposal.
\textsuperscript{2066} Amendment 158 introducing a new Article54a, Amendment 67 amending recital (97), European Parliament legislative resolution of 12 March 2014 on the proposal for a GDPR (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).
\textsuperscript{2067} Articles 51a and 54a and recitals 97, 97a, 97b and 97c of Consolidated version of the General Data Protection Regulation, in Council general approach (Council document 9565/15 of 11 June 2015).
\textsuperscript{2068} E.g., European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 237.
\textsuperscript{2069} E.g., Article 54a (4) of Consolidated version of the General Data Protection Regulation, in Council general approach (Council document 9565/15 of 11 June 2015).
\textsuperscript{2070} Some cases of enforcement cooperation – e.g. in relation to Google and WhatsApp - are explained in David Barnard-Wills & David Wright, Deliverable 1 – “Co-ordination and co-operation between Data Protection Authorities”, www.phaedra-project.eu.
of its members, but also of all internet users who come into contact with it.\textsuperscript{2071} One of the recommendations of the Belgian DPA was that Facebook should refrain from systematically using data of non-Facebook users,\textsuperscript{2072} since this practice breaches Belgian data protection law. This investigation was carried out in an informal cooperation with two other European DPAs (the Netherlands and the German State of Hamburg), but without involvement of the DPA of Ireland, the country where Facebook had its main establishment in the European Union. The Irish DPA had earlier investigated the practices of this company,\textsuperscript{2073} without concluding that a breach of Irish data protection law had occurred.\textsuperscript{2074} Not surprisingly, Facebook denied the applicability of Belgian data protection law and the competence of the Belgian DPA.\textsuperscript{2075}

The rationale behind this structured cooperation mechanism is the need for consistent enforcement of data protection rules across Europe, and also to prevent that multinational companies have to deal with divergent enforcement decisions. The mechanism also ensures that the multinational companies deal with the lead authority as their sole interlocutor.\textsuperscript{2076} The strong emphasis on the importance of the mechanism for private companies is confirmed by the link the Commission makes between the one stop-shop mechanism – and the consistency mechanism discussed below – and the digital single market.\textsuperscript{2077} The advantages for the protection of the individual – protection in an equal way, creating legal certainty, foregoing forum shopping by data controllers and processors choosing the perceived most lenient DPA\textsuperscript{2078} – seem to be of less importance, at least in the justification given by the Commission.

A consistency mechanism, but diverging views on its rationale

Another novelty of the Commission Proposal for a General Data Protection Regulation is a consistency mechanism that involves the EDPB, which must be set up under the regulation as the successor to the Article 29 Working Party. The EDPB, consisting of representatives of DPAs, is to play a formal role in the enforcement of EU data protection law, in contrast with the Article 29 Working Party, as was explained. This formal role may result in an opinion giving guidance to the DPAs and, ultimately, even in a binding decision. The Commission

\begin{itemize}
\item \textsuperscript{2072} Recommendation No. 04/215 of the Belgian Privacycommission of 13 May 2015, p.26.
\item \textsuperscript{2073} Further read: David Barnard-Wills & David Wright, Deliverable 1 – “Co-ordination and co-operation between Data Protection Authorities”, www.phaedra-project.eu, at 39-44.
\item \textsuperscript{2074} See Annual Report of the Data Protection Commissioner of Ireland 2014 published on its website.
\item \textsuperscript{2076} E.g., Article 51a (3) of Consolidated version of the General Data Protection Regulation, in Council general approach (Council document 9565/15 of 11 June 2015).
\item \textsuperscript{2077} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, COM (2012) 9 final, at 7-8.
\item \textsuperscript{2078} See on this section 2 above, with reference to E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CMLR 46 (2009), pp. 1395–1442, at 1412.
\end{itemize}
The EDPB does not include any binding powers for the EDPB. The positions of the European Parliament and the Council do introduce such binding powers, albeit limited to strictly defined circumstances that differ in the positions of the European Parliament and the Council.

The consistency mechanism is intended to apply to a number of situations, such as the situation where processing operations relate to “the offering of goods and services to data subjects in several Member States, or to the monitoring of their behaviour”. This scope of activity potentially extends to all activities on the internet within the European Union. This does not mean that all activities are finally scrutinised by the EDPB, but in all these cases the EDPB will be informed and it may be called upon to act. This mechanism – as amended during the legislative process – is a further instrument to regain control over data processing operations on the internet. The positions by the European Parliament and the Council limit the cases in which the EDPB may be involved.

The consistency mechanism proposed by the Commission aims at contributing to the mandate of Article 16 TFEU, in compliance with requirements of effectiveness. However, as the negotiations in the European Parliament and the Council reveal, the legitimacy of the envisaged mechanism raises questions relating to the absence of a communis opinio regarding its rationale.

The need for clear and uniform rules for businesses providing legal certainty and minimising the administrative burden was a reason for the Commission to propose the reform of the legal framework for data protection, which is expected to stimulate economic growth, create new jobs and foster innovation. The proposed regulation must do away with the fragmented legal environment resulting not only from divergences between the rules themselves, but also from the diverging control of the rules. This is the rationale of the internal market.

However, for the Commission the rationale of the consistency mechanism is wider and has two additional goals. First, consistency serves as a conflict-solving mechanism where the views of the DPAs in a specific case may possibly diverge. Second, consistency is intended as an instrument to ensure the correct and uniform application of the regulation within the wider territory of the European Union. The difference between these two goals is explained as follows. The first goal ensures that a specific processing operation – for instance an internet application – is not judged in divergent manners in the Member States

---

2079 Article 58 of the Commission Proposal for a GDPR, COM (2012), 11 final, only mentioning opinions.
2084 See in particular the procedure foreseen in Article 58(3) of the Commission proposal.
2085 See in particular the procedure foreseen in Article 58(4) of the Commission proposal.
and that the supplier of this application is confronted with one decision applicable in the whole European Union. The second goal must ensure that a decision taken is also consistent with decisions taken in other cases and hence contributes to the uniform (and correct) application of EU data protection law.\textsuperscript{2086} The second goal is connected to the obligation of DPAs to contribute to a harmonised and effective level of protection in the European Union, mentioned in the introduction of this chapter. In our view, the consistency mechanism would only succeed in neutralising the fragmented legal environment, as intended by the Commission, if both goals are achieved.

However, this is not the view taken in other contributions to the legislative process. To start with, the Article 29 Working Party is critical of the Commission proposal: the “mechanism should ensure consistency in matters only there where it is necessary, should not encroach upon the independence of national supervisory authorities and should leave the responsibilities of the different actors where they belong”.\textsuperscript{2087} The Working Party considers that the consistency mechanism should only be triggered where the DPAs do not reach consensus on the assessment of the case and/or measures to be taken.\textsuperscript{2088} This position underscores the first goal, mentioned above. The second goal does not seem relevant for the Working Party. This is also due to the fact that the Working Party is opposed to a role of the Commission in the procedure\textsuperscript{2089} and seeks to limit the caseload.\textsuperscript{2090}

The view that the consistency mechanism should be limited to cases of disagreements between authorities in a specific case seems to be shared by the European Parliament. One of the amendments of the European Parliament limits the consistency mechanism to cases of serious objections of an authority to a draft measure of another authority, the ‘lead authority’.\textsuperscript{2091} A similar approach is taken by the Council. In individual cases, relevant and reasoned objections and conflicting views may trigger the consistency mechanism.\textsuperscript{2092}

\textit{From the citizens’ perspective: the rationale behind a consistency mechanism is not clear}

\textsuperscript{2086} To be complete, the Commission proposal also foresees a role for the consistency mechanism in procedures not relating to individual cases, such as the adoption of a list of the processing operations subject to prior consultation and various procedures relating to the transfer of personal data to third countries (Article 58 (2)) of the proposal.\textsuperscript{2087} Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals - WP 191 (23.03.2012), at 20.\textsuperscript{2088} Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals - WP 191 (23.03.2012), at 20.\textsuperscript{2089} In the same sense, European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 248-255.\textsuperscript{2090} In the same sense, European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 245.\textsuperscript{2091} Amendment 167, introducing a new Article 58a, European Parliament legislative resolution of 12 March 2014 on the proposal for a GDPR (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).\textsuperscript{2092} Article 57 (3) (a) and (b) of Consolidated version of the General Data Protection Regulation, in Council general approach (Council document 9565/15 of 11 June 2015).
The need for uniformity of the control is not evident from the perspective of the exercise of the individual’s right to data protection. The Commission mentions “uneven protection for individuals” as an issue, but without further elaborating on it.

EU law requires that an individual is protected in an effective manner, but not that the level of protection is identical in all Member States or parts of Member States, despite the fact that the principle of equal treatment is widely interpreted under EU law. This principle even has the character of a constitutional norm, also because Article 20 Charter provides that everyone is equal before the law. This principle ensures that within the jurisdiction of a Member State there is equal treatment between that state’s own nationals and nationals of other Member States.

However, the principle of equal treatment does not ensure that the individual is entitled to expect that the enforcement of EU law is the same in each Member State, unless this is required by a specific arrangement under EU law. The standard formula in the case law is that enforcement of EU law by Member States should be effective, proportionate and dissuasive, meaning that enforcement is not necessarily identical in each Member State. The alternative view – enforcement should be harmonised or unified – would even be contrary to the principle of subsidiarity, as far as this expresses a preference for decision-making by the Member States.

Of course, individuals benefit indirectly from the uniformity of the control. Uniformity – provided it is based on a high standard of protection – ensures that weak enforcement practices are abolished. Chapter 7 of this study referred to existing inadequacies in the powers and resources of the DPAs. Moreover, a uniform enforcement renders forum shopping by data controllers – choosing the DPA of the country requiring the lowest level of compliance – meaningless.

However, this argument does not compensate for the fact that the proposed mechanism is not based on a clear view of its benefits for the exercise of the individual’s right to data protection. Had this been the case, this could have contributed to enhancing the legitimacy of the mechanism.

---

2096 Because of the prohibition of discrimination on grounds of nationality in Article 18 TFEU and in Article 21(2) Charter.
2098 On subsidiarity, see Chapter 4, Section 4.
2099 See Chapter 7, Section 11.
2100 See also Sections 3 and 5.
6. Experience in a Related Area: Governance in Electronic Communications through a Network of Authorities with a Task for BEREC to ensure Consistent Application

Electronic communications – or in the old terminology: telecommunications – is an example of a domain with a strong role for governance by European networks of regulatory agencies. This is, for different reasons, an interesting domain for the subject of this chapter not in the least because the Body of European Regulators for Electronic Communications (BEREC) served as a model for the consistency mechanism in the proposed General Data Protection Regulation.

Recital (3) of Regulation 1211/2009 establishing BEREC reveals the main dilemma, which will be elaborated upon, further in this chapter, in relation to the DPAs. On the one hand, the consistent application of the EU framework in all Member States is essential for the successful development of the internal market for electronic communications. The national regulatory authorities in electronic communications have as a task to contribute to the internal market, inter alia by cooperating with each other, so as to ensure consistency. On the other hand, national authorities must be granted flexibility to apply the rules in the light of national conditions. They remain national authorities, operating within the national jurisdictions.

This section explains relevant elements of the (legislative) history of BEREC, its main tasks and its relationship with the national authorities and the Commission. Supervision in the area of electronic communications is – under the model of Framework Directive 2002/21 (as amended by 2009/140) and Regulation 1211/2009 – a task of the national regulatory authorities. BEREC ensures the regulatory coordination and national authorities have to take the utmost account of the views of BEREC. BEREC itself is composed of a board of

---

2102 Commission Proposal for a GDPR, COM (2012), 11 final, at Chapter VII.
2104 To be complete, flexibility is only needed “in certain areas”. Zinzani explains that this recital reflects the conflicting views in the negotiations process, Marco Zinzani in: Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, Ch 7.
national regulators and has an unspecified institutional status. The recitals of Regulation 1211/2009 explain the status in the negative: it should neither be an EU agency nor have legal personality. BEREC is supported by the BEREC Office, an EU body with legal personality.

This institutional design reflects the legislative history where the Commission proposal to establish an EU agency – with a role going beyond providing just support – was rejected by the European Parliament and the Council for a number of reasons, including insufficient independence and accountability. The history of reticence in creating a European agency in the area of telecommunications goes further back, to the years 1990, and resulted back then in a network – the European Regulators Group – with very broad functions but very few powers. This reticence relates to various factors. The opposition of Member States was based on considerations of sovereignty, the wish to retain control over – sensitive – political issues and the unwillingness to fund an agency. Opposition against the creation of BEREC as an EU agency is also reported to have originated with national regulatory authorities, who favoured a network over an EU agency. These authorities have also sought to limit the powers of BEREC. The negotiations on the proposed General Data Protection Regulation display similar tendencies.

The mandate of BEREC aims at ensuring the consistent application of the EU regulatory framework for electronic communications and services, and thereby at contributing to the internal market in this field. BEREC should also serve as a body for reflection, debate and

---


2115 See David Coen and Mark Thatcher, Network Governance and Multi-level Delegation: European Networks of Regulatory Agencies, Journal of Public Policy, Vol. 28, Issue 01, April 2008, pp 49–71, at 55-56. One factor they mention, the risk of the treaties unravelling, is not discussed in main text because it is not relevant here.

2116 Coen and Thatcher mention universal service and national champions.


2119 An example is the limitation of the role of the EDPS, which was proposed by the Council, leading to a text in the General Approach where the EDPS was deprived of its voting rights in the EDPB and also the influence of the EDPS on the secretariat was restricted. See Articles 64 (4) and 71 of Council general approach (Council document 9565/15 of 11 June 2015). The Article 29 Working Party, composed of mostly national DPAs did not side with the EDPS in this debate.

2120 See on this framework also Chapter 6, Section 10 of this study.
advice to the EU institutions.\footnote{Recitals (8) and (9) of Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L (2009), 337/1.} The tasks of BEREC are of an advisory nature.\footnote{Article 3(1) of Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L (2009), 337/1.} However, the views of BEREC do carry a certain weight. The national regulatory agencies and the Commission “shall take the utmost account of any opinion, recommendation, guidelines, advice or regulatory best practice adopted by BEREC”.\footnote{Article 3(3) of Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L (2009), 337/1.} This is in particular the case where BEREC takes a position relating to the competition in the internal market and – more directly relevant for data protection – relating to the consistent application of remedies.\footnote{Articles 7 and 7a of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, as amended by Directive 2009/140.} The positions of BEREC are based on close cooperation between the national authorities with a strong focus on peer review and strict time limits.

This mechanism and in particular the obligation of the national authorities to take the utmost account of BEREC’s contributions gives the positions of this agency an authoritative – although not binding – status in the application of the EU framework for electronic communications. It is evaluated as being rather successful.\footnote{Study on the Evaluation of BEREC and the BEREC Office, carried out for the European Commission by PricewaterhouseCoopers, 2012, at 118-135.} However, there is one point of criticism in the functioning of BEREC that may be relevant for the cooperation of DPAs as well: BEREC is reported to be insufficiently focused on the EU perspective and on the EU-wide approach towards the issues addressed.\footnote{Article 59(2) of the Proposal.} This model – advice, plus the obligation to take the utmost account of this advice – served as inspiration for the proposed General Data Protection Regulation,\footnote{See mainly Articles 58(8) and 59(2) of the Commission Proposal for a GDPR, COM (2012), 11 final.} albeit in a modified fashion. The Commission proposal provides that a DPA should take account – not the utmost account – of the opinion of the EDPB. The Commission does not have any such obligation. On the contrary, in a specific situation, the national DPA must take the utmost account of the opinion of the Commission.\footnote{Article 59 is deleted in these contributions. European Parliament legislative resolution of 12 March 2014 on the proposal for a GDPR (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Council general approach (Council document 9565/15 of 11 June 2015).} This provision does not sit easily with the requirements of independence of DPAs, and is no longer included in the contributions of the European Parliament and the Council.\footnote{Article 59(2) of the Proposal.}

\textit{Conditions for effective cooperation inspired by the parallel with cooperation in EU competition law}

\footnote{Recitals (8) and (9) of Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L (2009), 337/1.}
The model of Regulation 1/2003 on the implementation of the rules of EU competition law,2130 with a self-standing enforcement power of the Commission based directly on Articles 101 and 102 TFEU, is not further explored in this study. The model it is too different from the present and future system of enforcement of EU data protection law. However, the model contains elements that help understanding the cooperation between DPAs in a composite administration and confirm the benefits of clear procedural rules.

Regulation 1/2003 introduces a model with national regulators applying EU competition law and a coordinating role of the European Competition Network, comprising the national competition authorities and the Commission.2131 Kloza & Moscibroda2132 analyse interesting parallels with data protection, as a basis for developing four conditions for effective cooperation. First, effective enforcement cooperation requires a clear, structured and sufficiently detailed legal basis. Second, it requires comprehensive forms and procedures. Third, the exchange of case-related information – which may be confidential and/or subject to data protection rules – must be enabled. Fourth, – but this exceeds the scope of the present chapter on intra-EU cooperation – effective enforcement cooperation in an internet environment requires a global reach.

7. Cooperation between DPAs in a Composite Administration, against the Background of Developing EU Administrative Law

Under EU law, DPAs are hybrid in character operating in between the Union and the Member States. They are part of an integrated or composite administration, based on a horizontal collaboration between administrative organs in a non-hierarchical manner.2133 This integrated or composite administration is the result of a trend in which the separation of duties between the European Union and the Member States becomes less clear and is complemented by forms of administrative cooperation. Administrative networks play an increasing role – in various constellations – in the implementation of EU law and policy, which is, in principle, a duty of the governments of the Member States.2134

2133 Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57, at 47.
The cooperation between DPAs fits within this trend. The fact that the DPAs have a special status as a result of their mandate based directly on primary EU law – Article 16(2) TFEU and Article 8(3) Charter – makes the need for cooperation even more imperative than in other areas of EU intervention.

This section contains a general theory on administrative cooperation under EU law, against the background of developing EU administrative law. The aim of this section is to provide the background for a better understanding of the cooperation mechanisms between the DPAs, from the perspective of an effective and legitimate cooperation.

Administrative cooperation under EU law as a matter of common interest

The integrated or composite administration under EU law is a phenomenon that involves EU authorities and Member State authorities, or authorities of more than one Member State that have distinct roles but are inter-dependent. This phenomenon includes composite decision-making procedures with the input of authorities from different jurisdictions, national as well as European. It is based on shared responsibility, not on a division of responsibilities, which is the main feature of a federal structure. As Bignami states: “Both national and European administrations share responsibility for single determination of rights and duties under European law.”

The integrated or composite administration has elements of horizontal and vertical cooperation. In practice, the demarcation between horizontal and vertical cooperation is fluid, as Harlow illustrates. She describes a system of multi-level governance with bottom-up mechanisms where EU objectives are achieved through mutual cooperation of authorities of the Member States and top-down mechanisms with a key role of EU bodies, but that are also based on transnational networks where national and EU bodies work together to carry out jointly agreed policies. Various forms exist.

This phenomenon of an integrated or composite administration is not laid down in the Treaties. However, there are links with primary EU law. Foremost, Title XXIV of the TFEU is titled “Administrative cooperation”. Article 197(1) TFEU provides that “Effective implementation of Union law by the Member States, which is essential for the proper functioning of the Union, shall be regarded as a matter of common interest.” The Union may

---

2135 Further read: Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57.


take action to support the Member States in this perspective, however without harmonising national laws and regulations.

Moreover, the cooperation between the partners in an integrated or composite administration is governed by the principle of sincere cooperation in Article 4(3) TEU which is considered to be a reflection of federal good faith.\textsuperscript{2140}

Furthermore, the right to good administration is recognised as a fundamental right in Article 41 Charter. Under Article 41(1) Charter “every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union”. Article 41(2) specifies the right to be heard, the right to have access to his or her file and the obligation of the administration to give reasons for its decisions. Article 41 Charter is connected to the notion that the European Union is subject to the rule of law\textsuperscript{2141} and to the right to an effective remedy under Article 47 Charter.\textsuperscript{2142} Although Article 41 of the Charter is only addressed to EU institutions and bodies, there are indications that the Court of Justice considers this a provision of general application binding on the Member States when they act within the scope of EU law.\textsuperscript{2143} The Court ruled in \textit{M.M.}, in relation to Article 41(2), that the provision is of general application.\textsuperscript{2144} Hence, the case law gives good arguments in support of the view that Article 41 applies to the actors in an integrated or composite administration. This covers the DPAs.

These provisions of primary law underline that the actors in an integrated or composite administration under EU law should act in the common interest. These actors have a shared authority and a shared responsibility under EU law. They should exercise their duties with a certain degree of care.\textsuperscript{2145} Finally, individuals are entitled to a good administration, which is closely linked to the duty of care of the administration. Craig refers to a principle of care or diligent or impartial administration.\textsuperscript{2146}

\textbf{Material aspects of the composite administration: mutual cooperation and mutual trust}

\begin{footnotesize}
\begin{itemize}
\item Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010, at 7-045.
\item Explanations relating to the Charter of Fundamental Rights, OJ (2007) 303/17, Explanation on Article 41.
\item Case C-277/11, \textit{M.M.}, EU:C:2012:744, at 84.
\end{itemize}
\end{footnotesize}
The actors in the composite administration cooperate in the common interest, but in a non-hierarchical manner, exercising their duty with a certain degree of care. Their mutual cooperation has different material aspects, all necessarily based on mutual trust. First, cooperation requires the application and enforcement of national rules by authorities in other jurisdictions, even in situations where these national rules are not in conformity with the law in the other jurisdiction. A requesting authority may expect that the requested authority cooperates, even in those cases. Second, cooperation requires the recognition of procedural standards and controls in other Member States. There is a rebuttable presumption that fundamental rights are protected in the requested Member State. Third, a requested authority must cooperate sincerely and dedicate sufficient resources to handling the request and not question the validity of the request. The requested authority also has an obligation to verify the assumptions it makes when it reports on a request.

This is all linked to the concept of mutual recognition, a concept that developed in EU law in the context of the internal market and implies that Member States must recognise each others' tests, diplomas and evidence, for instance in relation to professional qualifications. Mutual recognition plays a central role in the area of police and judicial cooperation in criminal matters. In the area of data protection, too, examples can be found of mutual recognition in the relation between DPAs. One example is the cooperation between the DPAs on the transfer of personal data based on Binding Corporate Rules, as developed by the Article 29 Working Party. Where one DPA approves a specific transfer to a third country on this basis, other DPAs must recognise this without further scrutiny.

Mutual recognition is based on trust. As Den Heijer states: “if the system of mutual recognition is to work, there must also be complete mutual confidence in police and judicial systems in the Member States. High standards not only must be attained, but also must be maintained.”

---

2147 Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57, at 47.
2150 Under Joined cases C-411/10 and C-493/10, N.S., and M.E. and Others, EU:C:2011:865.
2151 Under Case C-503/03, Commission v Spain, EU:C:2006:74.
Networks of cooperation and mechanisms for institutional cooperation are instrumental to enhancing trust and, by doing so, facilitating cooperation, for instance by developing common administrative standards. The duty to cooperate and mutual trust are linked to the principle of sincere cooperation under Article 4(3) TEU. As a result, these networks and mechanisms must exercise their own duties in accordance with high standards of confidence in respect of the principle of sincere cooperation. In a composite administration, the cooperation between the various actors and levels is a condition for success.

The requirements of sincere cooperation are even higher in the context of internet privacy and data protection, due to the presumed lack of government control. The principle of sincere cooperation under Article 4(3) TEU applies to all governmental actors (EU and national) involved in the implementation of EU law and policies in this domain. Arguably, the principle of sincere cooperation extends to cooperation with authorities in related policy areas, where they deal with aspects of privacy and data protection. Cooperation in the domain of privacy and data protection on the internet also involves non-governmental stakeholders. Where DPAs cooperate with actors outside government, the latter should respect principles of good governance, but Article 4(3) TEU does not apply to non-governmental stakeholders.

Procedural standards applied in the composite administration should ensure accountability

The composite administration involves a “multi-jurisdictional nature of many of its procedures and a pluralization of the actors involved”. This requires a high degree of procedural cooperation, based on a clear legal relationship between the various actors. Also where the responsibilities are shared clear rules are needed, to enable accountability. Rules on administrative procedure should be designed to maximise the two objectives of public law: the effective discharge of public duties and the protection of individuals’ rights. Arguably, a good administration as meant in Article 41 Charter should meet both objectives.

Harlow argues that a composite administration requires a networked response from administrative procedural law, in what she calls “Accountability Networks”. She states that “Governance outside the state” must be countered by administrative law, providing for multi-dimensional accountability. She mentions as examples the collaboration of courts and the information sharing and advisory cooperation by national parliaments, which results from the responsibilities of national parliaments for EU law recognised in the Treaties. She also mentions the cooperation within the European Network of Ombudsmen.

---

Procedures must ensure effective remedies in multi-jurisdictional cooperation between authorities, also as a prerequisite for mutual trust. Procedural standards, such as transparency, justification and inclusiveness, contribute to legitimacy. Procedural legitimacy is considered as a compensation for flaws in the democratic accountability.\textsuperscript{2161}

Hofmann & Tidghii mention two procedural standards that are particularly relevant in a composite administration. The administration must, first, be capable of ensuring that it can rely – under the rule of law – on accurate and lawfully collected information and, second, the right to fair hearing must be respected.\textsuperscript{2162} The first standard played a role in \textit{Commission v Spain}\textsuperscript{2163} on the Schengen Information System. An authority of a Member State could not base a decision on an act of an authority in another Member State, without first verifying the accuracy of the information on which the decision was based. The Court of Justice required the second standard in \textit{Technische Universität München},\textsuperscript{2164} in relation to the duty of the competent institution to examine carefully and impartially all the relevant aspects of the individual case.\textsuperscript{2165} Both standards relate to the fact that, in a composite administration with various actors, the information may be dispersed. These procedural standards must compensate for this shortcoming.

Moreover, information exchange is a key instrument for a well-functioning European composite administration. That is why informational networks were created in various policy areas, allowing all actors in a composite procedure to have access to information necessary for decision-making.\textsuperscript{2166} An example is the Internal Market Information System (IMI), which was conceived as a mechanism to exchange information, to facilitate cooperation amongst national authorities and between national and EU authorities, for the purpose of better decision-making.\textsuperscript{2167} More generally, information exchange plays a central role in discussions on EU administrative law.\textsuperscript{2168}

\textit{Fragmentation of areas of law as a further complication, also in view of the special status of DPAs}

\textsuperscript{2161} W. Vandenbruwaene, Multi-Level Governance through a Constitutional Prism, Maastricht Journal of European and Comparative Law 2014, Volume 21, nr 2, at 229-242, at 241.
\textsuperscript{2163} Case C-503/03, Commission v Spain, EU:C:2006:74, at 52-55.
\textsuperscript{2164} Case C-269/90, Technische Universität München, EU:C:1991:438, at 13-14. This case is also relevant in relation to the duty of care.
\textsuperscript{2165} This is closely related to the principle of care or diligent or impartial administration, referred to by Craig.
\textsuperscript{2167} Lottini, Micaela, “An Instrument of Intensified Informal Mutual Assistance: The Internal Market Information System (IMI) and the Protection of Personal Data”, European Public Law 20, No.1 (2014), 107-126.
\textsuperscript{2168} See the documents published by Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure.
Fragmentation of EU administrative law is a complicating factor. The rules and procedures under EU law are quite often sector-specific or issue-specific. The example of data protection illustrates this, in particular after the entry into force of the General Data Protection Regulation, when cooperation mechanisms of DPAs will exercise powers in individual cases. A procedure before a cooperation mechanism of independent DPAs has no equivalent in other areas of EU law. A further complication is that the competences in related areas may be on different levels. As discussed in this study, the competence of the European Union under Article 16 TFEU is unique under EU fundamental rights law. A procedure before a cooperation mechanism of independent DPAs may have an impact on a procedure under national law, in relation to the exercise of another fundamental right.

A resolution of the European Parliament states that the absence of a coherent and codified set of administrative law makes it difficult for citizens to understand their rights. Procedural guarantees – such as those included in the ReNEUAL Model Rules on EU Administrative Procedure – could deal with the disadvantages of fragmentation of administrative law in the European Union, and also cover procedures in the area of data protection.

8. Three Models to Organise Cooperation between DPAs, against the Background of the Proposed GDPR

The previous sections discussed three types of cooperation on enforcement, namely the exchange of information between DPAs, the effective assistance in supervision as well as the carrying out of joint investigative tasks. Presently, the Article 29 Working Party only contributes indirectly to enforcement activities by exercising its advisory role, which it interprets in a wide manner.

The proposed General Data Protection Regulation will bring considerable novelties by introducing a one-stop shop mechanism with a lead authority and a consistency mechanism. The one-stop shop mechanism is meant to strengthen the protection of the individual although it is mainly justified by internal market considerations, at least by the Commission, whereas the consistency mechanism with the EDPB is based on a rationale that is not fully shared between the EU institutions. For the Commission it is an instrument for the uniform application of EU data protection law, whereas for the European Parliament and the Council it is mainly a conflict solving mechanism.

The three models discussed in this chapter do not fully coincide with the mechanisms introduced by the proposed General Data Protection Regulation. The one-stop shop mechanism with a lead authority is a specification of the first model (cooperation by DPAs),

---

2170 European Parliament resolution of 15 January 2013 with recommendations to the Commission on a Law of Administrative Procedure of the European Union (2012/2024(INL)).
but it also has elements of the second model (a structured network), if only because of the role of the EDPB in deciding which DPA is competent.\textsuperscript{2172} The envisaged consistency mechanism has elements of the second model (a structured network) and the third model (a European DPA).

The example of electronic communications – including BEREC – shows the difficulties in accepting a role of the central European level, leading to a model where national authorities shall take the utmost account of opinions of BEREC, a model that served as inspiration for the General Data Protection Regulation.

The integrated or composite administration in the European Union comprises horizontal as well as vertical cooperation between authorities. This type of administration is characterised by considerations of common interest, good faith and good administration. Material aspects of the composite administration comprise mutual cooperation and mutual trust. Procedures of administrative law are, in our view, an appropriate instrument to compensate for flaws in the democratic legitimacy. This means precise rules, also on procedure and on the exchange of case-related information.\textsuperscript{2173} A problem is the fragmentation of procedures in various areas of law.

\textit{Introduction of the three models of cooperation}

The following sections describe three models of cooperation: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models are examples of the integrated or composite EU administration where competences are not divided but shared. The main differences between these three models relate to the nature of coordination.

In the first model, the emphasis is on the horizontal cooperation. The two objectives of cooperation are achieved solely on the basis of a bottom-up approach, without any centralised structure. Horizontal cooperation of DPAs enhances the legitimacy of the control, because it emphasises political as well as public democratic accountability at the level of the Member States.

The two other models are more vertical in character with a top-down approach in which an EU network or an EU body determines policies,\textsuperscript{2174} although decision-making is often based on consensus between the partners. An important difference between the second (a structured

\textsuperscript{2172} Amendment 158, Article 54(a)(4), European Parliament legislative resolution of 12 March 2014 on the proposal for a GDPR (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Article 57 (3) (a) and (b) of Consolidated version of the General Data Protection Regulation, in General approach of the Council, Council general approach (Council document 9565/15 of 11 June 2015).

\textsuperscript{2173} See Section 6 above, referring to Dariusz Kloza and Anna Moscibroda, Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law, International Data Privacy Law, 2014, Vol. 4, No. 2, at 135-137.

network) and the third model (a European DPA) lies in the decision-making structure: the second model only leads to consensual decisions, ensuring that each national authority remains effectively responsible vis-à-vis its residents and the judiciary; the third model is based on the notion that effective privacy and data protection in an internet environment requires a decision-making structure that may overrule a national authority.

This study presents the three models as complementary. The three models compose a layered structure for an independent, effective and accountable control of EU data protection. An important notion behind this layered structure is the principle of subsidiarity, in this context referring to decisions taken as closely as possible to the citizen. Issues that can be addressed by horizontal cooperation between DPAs should remain at that level, if this is not the case issues should be addressed by a structured network of DPAs, and only if the latter option is not sufficient is there need for involvement of a European DPA.

9. The First Cooperation Layer: Horizontal Cooperation between DPAs

The essence of horizontal cooperation

The first layer of enforcement cooperation is the horizontal cooperation between DPAs, without a structured network laid down in law. Horizontal enforcement cooperation is essentially bilateral, with the aim of ensuring that the DPAs, which have a stake in a specific data processing operation with cross-border elements, work together in an efficient and effective manner. This stake can be the consequence of the fact that a data subject, a data controller or data processor has his residence in the Member State where the DPA is established or that the data are stored in this Member State. It may also happen that multiple DPAs need to investigate and prosecute similar or even identical issues as a result of overlapping jurisdictions. In these cases, cooperation results in an efficient use of resources, inter alia by avoiding duplication of effort.

An essential feature of horizontal cooperation is the absence of hierarchy. The cooperation is characterised by sharing of responsibilities, a common interest, good faith and good administration. In an internet environment horizontal cooperation can be limited to two DPAs. This was the case in Weltimmo, where only the Hungarian and the Slovak DPA were involved in relation to a data controller based in the Slovak Republic who was offering services through the internet in Hungary.

However, horizontal cooperation involves all DPAs concerned. Where goods or services are offered on the internet without territorial fragmentation, this can be the DPAs of all 28

2175 [Article 5(3) TEU.]
2176 [David Barnard-Wills & David Wright, Deliverable 1 – “Co-ordination and co-operation between Data Protection Authorities”, www.phaedra-project.eu, at 7.]
2177 [As explained above in Section 7.]
2178 [Case C-230/14, Weltimmo, ECLI:EU:C:2015:639.]
Member States. Generally speaking, horizontal cooperation between concerned DPAs is not sufficient to meet the objectives of cooperation in an internet environment. Horizontal cooperation should lead to a decision-making procedure where all DPAs are entitled to give their views. Within a structure of horizontal cooperation, enforcement decisions should, in principle, only be taken on the basis of consensus between the DPAs of all 28 EU Member States. This is obviously not a satisfactory perspective from the point of view that internet privacy and data protection require swift and effective responses.

**Developments towards a closer regime for horizontal cooperation with precisely formulated rules**

Horizontal cooperation between DPAs should be framed in such a way as to ensure effective cooperation, at the same time taking into consideration requirements of independence and judicial and democratic accountability.

In the first place, a closer regime would be useful in light of the developments in the information society where enforcement cooperation between DPAs in many cases is becoming the rule rather than the exception. The need for a closer regime is also the consequence of the inclusion of the control of the compliance with data protection rules in primary EU law, mandating the DPAs with the duty to ensure compliance. A closer regime of cooperation is in line with the developing integrated administration within the European Union where powers are shared. This sharing of powers may result in a situation where a DPA is no longer sovereign in taking decisions within its jurisdiction in individual cases, because the cooperation as laid down by law requires decisions to be taken by another DPA or, as discussed in the next section, by an institutional cooperation mechanism.

The one-stop shop mechanism proposed for the General Data Protection Regulation is an example of a closer regime. In this mechanism, a DPA can become dependent on a decision taken by a DPA in another Member State, even where the decision concerns the protection of individuals within its own jurisdiction. This is the essence of the introduction of the concept of a lead authority in EU law, as suggested by the European Parliament and the Council.

Section 5 above underlined that the one-stop shop mechanism has a strong link with the digital single market and also strengthens the effectiveness of the enforcement of data protection law within the European Union. Not everyone shares the view that the mechanism is necessarily advantageous to the individual who is entitled to protection. The Legal Service of the Council even expressed the opinion that the mechanism is essentially in the interest of businesses rather than in the interest of the data subject whose right is infringed.

---

2179 Article 16 (2) TFEU and Article 8 (3) Charter.
French DPA (CNIL), too, has expressed concerns in relation to the one-stop shop mechanism. As Raynal explains, the mechanism “would limit the ability of national DPAs to protect citizens effectively” and “impose the citizen to exercise their recourse action before a foreign court”.

This criticism is in line with the argument that the one-stop shop – at least in the version proposed by the Commission – involves the exclusive competence of one DPA. This may also provoke forum shopping by data controllers and processors locating their main establishment within the European Union in a Member State where the enforcement is (perceived as being) weak.

Precisely formulated rules providing procedural guarantees for the data subject could address this criticism. A closer regime of cooperation would also avoid competition between authorities as a result of overlapping jurisdictions.

**Procedural guarantees as compensation for democratic accountability**

Procedural guarantees are related to the right to good administration laid down in Article 41 Charter. This right includes the right of every person to be heard before any individual measure that would adversely affect him or her is taken, the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy, as well as the obligation of the administration to give reasons for its decisions (Article 41(2) Charter).

Procedural guarantees apply to DPAs when they operate within their national jurisdictions, on the basis of national administrative law. Moreover, this study argues that the DPAs as actors in an integrated or composite administration are bound by Article 41 Charter, in line with the ruling in *M.M.* Furthermore, the Member States should respect Article 41 Charter where they lay down rules for the establishment and functioning of DPAs, as required by Directive 95/46 on data protection.

However, where DPAs cooperate it should be specified which procedural guarantees apply and, in order to facilitate the cooperation, it makes sense to further specify the guarantees at

---

2182 Raynal in Carine Dartiguepeyrou (ed.), The Futures of Privacy, Cahier de prospective, Think Tank Futur Numérique, at 72.
2183 Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation, Paolo Balboni, Enrico Pelino, Lucio Scudiero, Computer law & security review 30 (2014) 392-402.
EU level. Examples of specified procedural guarantees can be found in the ReNEUAL Model Rules on EU Administrative Procedure.\textsuperscript{2189}

The effectiveness of remedies is an issue that requires specific attention in the composite administration in which the DPAs operate. A good example of the complexity is the procedure for complaints. It is the task of the DPAs to hear complaints of individuals, but the DPAs do not necessarily have jurisdiction for taking an effective decision on the complaint, in cases where the company against whom the decision needs to be enforced is not established within the national borders of the Member State, where the DPA is established. Procedural guarantees – as included in the ReNEUAL Model Rules on EU Administrative Procedure – could empower the individual to effectively invoke his rights also in this situation.

Obviously, precise procedural rules surrounding the horizontal cooperation of DPAs facilitate the judicial accountability. A closer regime with precisely formulated rules would also compensate for flaws in the democratic accountability of a horizontal cooperation mechanism. Procedural guarantees could enhance the democratic accountability, indirectly through general requirements of transparency, and more directly through reporting mechanisms to majoritarian bodies,\textsuperscript{2190} on the horizontal cooperation.

\textit{How to ensure that DPAs give sufficient priority to horizontal cooperation}

Guarantees must exist to ensure that resources are dedicated to cooperation and that priority is not given to national preoccupations. As explained above, cooperation is a means to ensuring that resources are used in a more efficient way, because it allows DPAs to join forces and avoids double work. However, it is not obvious that this is the perspective in which requests for cooperation are assessed in practice. When a request arrives, especially for complicated (technical) investigations, resources should be made available. Legal instruments can provide guarantees, for instance because they oblige a DPA to cooperate and specify the general obligation of sincere cooperation under Article 4(3) TEU. Additionally, a culture of cooperation is developing, for instance based on the successes of informal procedures of cooperation. An example is the informal cooperation coordinated by the French DPA on the investigation of the privacy policy of Google (2012-2014).\textsuperscript{2191}

\textbf{10. The Second Cooperation Layer: A Structured Network of DPAs, taking the Article 29 Working Party as an Inspiration to move ahead}

\textsuperscript{2189} Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure: Introduction to the ReNEUAL Model Rules /Book I – General Provisions, online version 2014; Book V - Mutual Assistance; Book VI- Administrative Information Management.

\textsuperscript{2190} See Chapter 7, Sections 13 and 14.

\textsuperscript{2191} As described by David Barnard-Wills & David Wright, Deliverable 1 – “Co-ordination and co-operation between Data Protection Authorities”, \url{www.phaedra-project.eu}, at 25-34.
The second layer of cooperation consists of a structured network of DPAs. Under present EU law, the Article 29 Working Party has a central role in this structured network. As explained above,2192 the contribution of the Working Party consists of non-binding, soft law instruments aimed at harmonisation in a non-coercive way, contributing to the uniform application of the national rules adopted pursuant to Directive 95/46 on data protection. Its task relates to the second objective of cooperation, mentioned above: the uniform interpretation of EU data protection law. The Working Party has no direct task in connection with the first objective: ensuring cross-border protection. This will change under the General Data Protection Regulation, which will replace the Article 29 Working Party by the EDPB.

Structured networks of expert bodies are a well-known phenomenon in the European Union, as may be illustrated by the example of the electronic communications sector. Coen & Thatcher explain these structured networks as being the result of different patterns of delegation.2193 Initially, there were two parallel tendencies: the delegation of tasks of the Member States to the European Union and the delegation of tasks within the Member States to expert bodies. This was followed by a further round of delegations to networks of expert bodies, triggered by the need for coordination in the internal market. These networks perform tasks delegated by the national expert bodies and also by the Commission.2194

This explanation is interesting for the Article 29 Working Party (and other structured networks of DPAs), although the constitutional position of DPAs under EU law is different from the status of most other expert bodies – such as the regulatory agencies described by Coen & Thatcher – and the DPAs do not exercise their tasks by delegation from the national governments or the Commission.

The parallel is the following: in the area of privacy and data protection there also was an initial shift in responsibilities – the term delegation is avoided on purpose – from the Member States to the European Union, in particular through the adoption of Directive 95/46. Independent DPAs were first set up within the Member States to take up the control of data protection. In some Member States the DPA already existed before the adoption of Directive 95/46.2195 The shift consists of the assumption of tasks by the network of DPAs, at present the Article 29 Working Party. The Working Party provides for non-compulsory harmonisation through the exercise of its advisory tasks and is only indirectly involved in enforcement.2196

The network of DPAs is expected to further evolve under the General Data Protection Regulation, with an EDPB assuming (certain) enforcement tasks. The cooperation of DPAs as expert bodies should also enhance the uniform application of EU data protection law within the European Union. The cooperation mechanisms give effect to the task of DPAs to

2192 See Section 4 above.
2194 Coen and Thatcher call this “upwards” and “downwards” delegation.
2195 See Chapter 7, Section 3.
2196 See Section 4 above.
contribute to the control in the entire European Union, but they are also an expression of democratic legitimacy, close to the citizen.

Development towards a closer structured network of DPAs

Bignami notes that little powers have been transferred to the Article 29 Working Party as the network of DPAs. She claims that one of the preconditions for the transfer of powers was not fulfilled, namely the existence of common preferences amongst the Member States on the substance of privacy policy.2197 She gives as an example the difference of views between the United Kingdom and France at the time of the negotiations in the Council on what became Directive 95/46 on data protection. According to Bignami, the United Kingdom opposed the strong views of France on informational privacy, emphasising other values like the freedom of expression and effective administration.2198

Arguably, the preferences on data protection have converged, as a result of 20 years of cooperation in the Article 29 Working Party, of harmonised approaches through soft law instruments and of common threats to privacy and data protection, such as big data and mass surveillance. This convergence paves the way for the transfer of further powers to a closer structured network of DPAs in the General Data Protection Regulation.

At present, the network is not close, despite the important advisory role of the Article 29 Working Party in the governance of data protection in the European Union. To mention an example of the loose network: under Article 29(2) of Directive 95/46 the Working Party is composed of representatives of one DPA of each Member State, but the representatives are not required to participate. Under Directive 95/46, the DPAs do not have any other legal obligation vis-à-vis the Working Party either.

The EDPB is meant to be an instrument for more efficient cooperation, obliging regulatory authorities to cooperate within the European structures, but also adding a further layer of complexity. The EDPB will have a task in providing guidance on general matters. This task is not contested and does, in itself, not complicate the situation. It is a continuation of the work of the Article 29 Working Party that it is intended to replace. This is also the way the European Union often works: experts from the Member States sit together and give guidance. This is an effective way of informal harmonisation of the application of EU law and is practiced in a large number of areas. There may, however, be some competition with the role of the Commission as the guardian of the Treaties.

What makes it more complicated is that the EDPB will have a task in the enforcement in individual cases. This task may be advisory (to give wider expertise, assisting the DPA in charge), more coercive (aimed at reaching consensus; the formula in which the DPA in

charge has to take the utmost account of the opinion of the EDPB as foreseen in the
Commission proposal), binding upon a national DPA or even taking over decision-making
powers. As was explained above, limited binding powers for the EDPB are included in the
contributions of the European Parliament and the Council to the legislative process.\textsuperscript{2199}

*The relation between the duties and powers of a structured network and the requirements for
composition and decision-making structures*

Where stronger duties and powers are given to a structured network of national authorities the
requirements in relation to the composition and decision-making structures should be stricter.
The stronger duties and powers the network has, the more it will be exercising elements of
the tasks of the authorities it is composed of, with the consequence that the network itself will
have to comply more with the requirements of independence, effectiveness and
accountability.

Fairly light requirements are acceptable where the involvement of a structured network is
limited to coordination, planning and guidance through soft law instruments, in short the
current tasks of the Article 29 Working Party. The requirements are higher where the network
plays a role in the enforcement in individual cases. The highest requirements apply where
decision-making powers are given to the structured network. In this latter option, the network
has features of a European DPA, which will be the subject of the next section.

*Composition of structured networks with senior representatives of DPAs and consensual
decision-making enhances legitimacy*

The structured networks within the European Union are often composed of senior
representatives of regulatory authorities. Where EU agencies are set up, a common
construction is to have two boards: a management board composed of representatives of
ministries\textsuperscript{2200} and a regulatory board with representatives of national regulatory authorities.
This is, for instance, the case in the field of financial supervision.\textsuperscript{2201} The regulatory board of
BEREC consists of the head or nominated high-level representative of the national
authorities.\textsuperscript{2202} However, interestingly enough the management committee of BEREC is
composed of the same group of representatives.\textsuperscript{2203}

A structured network of DPAs is slightly different, since the requirement of independence
precludes the setting up of a management board of representatives of the national ministries.

\textsuperscript{2199} See Section 5 above.
\textsuperscript{2200} See Chapter 7, Section 6 of this study.
\textsuperscript{2201} Mark Thatcher. The creation of European regulatory agencies and its limits: a comparative
November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and
the Office, OJ L (2009), 337/1.
\textsuperscript{2203} Article 7(1) of Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25
November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and
the Office, OJ L (2009), 337/1.
The Article 29 Working Party is composed of senior representatives of DPAs, normally the heads of the national DPAs,\textsuperscript{2204} although this is not required by Directive 95/46. This composition and the actual involvement of leaders of DPAs in the network connects the EU level with the national level, and is intended to contribute to the effect that the positions of the network have on the application of EU data protection law on the national level. It enhances the legitimacy of the network.

Consensual decision-making is an element in many structured networks in the European Union. Authorities deliberate with their peers in an endeavour to reach consensus. This makes the authorities to a certain extent accountable to these peers.\textsuperscript{2205} Another method to enhance legitimacy is to require a qualified majority for the decision-making, as has been done in the case of several networks of regulatory agencies.\textsuperscript{2206} For example, the regulatory board of BEREC normally acts by a two-thirds majority of its members.\textsuperscript{2207}

The rules of procedure of the Article 29 Working Party do not make any reference to consensual decision-making or a required qualified majority. Decisions are taken by simple majority. However, all members may request that their views are included in the decisions.\textsuperscript{2208}

The Commission Proposal for a General Data Protection Regulation requires neither a qualified majority, nor consensus in the EDPB.\textsuperscript{2209} However, the contributions of the European Parliament and the Council to the legislative process include provisions requiring that decisions in individual cases by the EDPB be taken by a two-thirds majority.\textsuperscript{2210} Moreover, these contributions aim at avoiding that individual cases are too often stepped up to the EDPB. Therefore, the lead supervisory authority has to cooperate with the other concerned supervisory authorities “in an endeavour to reach consensus”.\textsuperscript{2211} Furthermore, the various provisions that require taking account of or taking utmost account of the positions of

\textsuperscript{2204} List of members available on http://ec.europa.eu/justice/data-protection/article-29/structure/members/index_en.htm
\textsuperscript{2209} Article 58(7) of Commission Proposal for a GDPR, COM (2012), 11 final, mentions a simple majority of the members of the EDPB.
other entities may be seen in the light of the goal of reaching consensus, instead of determining that the position of one entity binds the other.

The consensual decision-making process ensures the widest support for the positions of the structured network of authorities. However, it also carries risks from the perspective of democratic accountability, as has been explained by Curtin. Representatives of authorities deliberating with their peers may become socialised and may strive to reach consensus within the network of experts without taking other perspectives into account. This carries the risk that they do not take national interests into account.

This is not necessarily a negative development in view of the importance of consistency of the decision-making in an internet environment. However, this development also may increase the fragmentation of EU policies by not taking other fundamental rights and societal interests sufficiently into consideration in a comprehensive manner. Furthermore, the lack of openness of consensual decision-making processes is a risk from the perspective of democratic accountability.

The role of the Commission in the structured network: how to combine two contradicting demands

It is beyond doubt that structured networks of national authorities – or a European DPA – assume responsibilities closely connected to the role of the Commission as the guardian of the treaties. The establishment of European networks and agencies was mentioned as a solution for problems in the implementation of EU law in the Member States with a view to improving the application and enforcement of EU law across Europe. The Commission assumes a big role in the functioning of EU agencies, also to promote agencies focusing on the EU perspective, which, as was explained in relation to BEREC, is not self-evident.

This role of the Commission is not easily to reconcile with the autonomy of agencies.

---

2217 M. Keading & E.W. Versluis in: Everson, Michelle, Cosimo Monda, and Ellen Vos (eds), 2014, EU Agencies in between Institutions and Member States, Kluwer Law International 2014, Chapter 4, e.g. at 74.
This role is even more complicated in relation to networks of independent DPAs. On the one hand, the Commission is the natural ally of the structured networks of DPAs that must ensure the consistent application of EU data protection law. On the other hand, independence, as interpreted by the Court of Justice as the absence of “any direct or indirect external influence on the supervisory authority”, excludes influence from the executive branch of government. In Commission v Austria, the Court of Justice specified that a right of the executive to be informed of the activities of a DPA may be incompatible with the requirement of independence, inasmuch as this right covers all aspects of the work of the DPA and is unconditional.

Hence, a close relationship between the Commission and the structured network of DPAs is desirable from the perspective of consistency. The network would benefit from a strong information position of the Commission. However, direct influence on the decision-making process should be avoided. There is a thin line between both effects.

As was explained above, the requirements of independence are stricter where the network plays a role in the enforcement in individual cases. From this perspective, the status quo under Directive 95/46 would be in line with the independence of DPAs and the independence of the Article 29 Working Party itself, as stipulated by Article 29(1) of the directive. Under this directive, the Commission is a member of the Article 29 Working Party, albeit without voting rights. It also provides the secretariat. These roles of the Commission – a part of the executive branch – do not fit naturally within the independence of the Article 29 Working Party, but they are not per se in contradiction with EU law.

It is not self-evident that these roles can be continued under the regime of the General Data Protection Regulation, although this will depend on the powers the EDPB will assume under this regulation. The Commission proposal limits the role of the Commission to the right to participate in the activities and meetings of the EDPB. However, this right is not subject to any conditions. It is questionable whether this right of the Commission is in line with the case law of the Court of Justice, as was explained above. An unconditional right to participate in the activities and meetings goes even further than an unconditional right to be informed, which the Court did not accept in Commission v Austria.

Furthermore, the Commission proposal includes more invasive mechanisms for influencing the independence of the EDPB; in particular it provides for the Commission suspending certain decisions of the EDPB. These mechanisms – heavily criticised and removed by

---

2219 Case C-518/07, Commission v Germany, EU:C:2010:125, at 19.
2220 Case C-614/10, Commission v Austria, EU:C:2012:631, at 62-64.
2223 E.g., European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package; Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals - WP 191 (23.03.2012).
the European Parliament and the Council\textsuperscript{2224} – would not fulfil the requirements relating to the independence of DPAs.

**Procedural guarantees**

What was observed above on procedural guarantees in relation to the horizontal cooperation of DPAs applies *mutatis mutandis* to a structured network of DPAs. Procedural guarantees are linked to Article 41 Charter on the right to good administration. Specification of the guarantees may be needed, also to make up for flaws in democratic accountability.

However, a structured network of DPAs requires specific procedural rules for two additional reasons. First, national administrative law does not apply to structured networks set up under EU law. Therefore, an EU instrument should lay down a full set of procedural guarantees in the absence of general rules of EU administrative law. Second, in a structured network, the responsibility for opinions and decisions may be of a hybrid nature and may not necessarily be clear. As was explained above, responsibilities are shared, not divided.\textsuperscript{2225} However, a clear division of responsibilities enhances democratic accountability, whilst it is even the basic condition for an effective remedy under the rule of law. By way of illustration, a provision requiring a national DPA to take account of an opinion of the EDPB may lead to legal uncertainty.\textsuperscript{2226} Where an individual challenges the decision of a national DPA, the latter can refer the responsibility to the EDPB.

More generally, procedural guarantees – such as included in the ReNEUAL Model Rules on EU Administrative Procedure\textsuperscript{2227} – could also empower the individual to invoke his rights in this situation in an effective manner.

### 11. **The Third Layer where Independence must be Ensured: Cooperation within a European DPA**

**The essence of cooperation within a European DPA**

The third model of cooperation of DPAs consists of a structured network that itself qualifies as a DPA, because it exercises tasks of the DPAs to ensure compliance with the data protection rules of the European Union. In this model, the network of cooperating DPAs is transformed into a European DPA. This model does not exist under Directive 95/46. There


\textsuperscript{2225} See Section 2 above.

\textsuperscript{2226} As in Article 58 (8) of Commission Proposal for a GDPR, COM (2012), 11 final.

\textsuperscript{2227} Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure, Article VI-39.
are however examples of this model under current EU data protection law in specific domains, namely the Joint Supervisory Bodies for Europol and Eurojust.2228

The result of the data protection reform may be that the envisaged consistency mechanism will contain elements of a European DPA, in particular where decision-making powers are given to the EDPB.2229 To be more precise: the EDPB will, depending on its powers and duties, have features of an EU body, functioning within the EU legal structure, although the EDPB will be (mostly, the EDPS will also be a member)2230 composed of representatives of national authorities.

Under these conditions, the EDPB would – in the exercise of these powers – no longer qualify as a structured network of national authorities. To the extent that the EDPB, as an EU body, has binding powers to ensure the compliance with data protection rules, it qualifies as a DPA within the meaning of Article 16(2) TFEU and Article 8(3) Charter. Under these circumstances, the EDPB must fulfil the requirements of independence as laid down in the case law of the Court of Justice.2231

Hence, a first requirement of a model of cooperation that includes elements of a European DPA is that its independence must be guaranteed, similarly to the independence of the (national) DPAs and under the same conditions laid down in the Courts’ case law.

A role of the EDPB as a European DPA should be considered from the perspective of the principle of subsidiarity. This role has advantages and disadvantages. In theory, a European DPA is the best way to ensure the functioning of the internal market, and to ensure the efficiency of the protection. This also creates legal certainty, since the judicial review would be a task for the Court of Justice of the European Union, applying EU law. However, a European DPA is not necessarily best placed to consider national specificities or to carry out the balancing with other fundamental rights and essential interests of Member States in an area that is closely linked to core tasks of Member States to protect (other) fundamental rights and to ensure the security of its citizens.2232 Considerations of democratic legitimacy and accountability plead against giving decision-making powers in individual cases to the EDPB.

Against this background, the model of European agencies, as described in Chapter 7 of this study, can be of help. A key feature of the European agency is that it operates in between the Union and the Member States.2233 The Member States have a guaranteed influence on the performance of the agency, for instance because the management board of the agencies is

---

2228 See Section 4 above.
2229 A good example of a decision-making power for the EDPB is found in Article 58 (a) of Consolidated version of the General Data Protection Regulation, Council general approach (Council document 9565/15 of 11 June 2015).
2230 In the Commission proposal and in the legislative resolution of the European Parliament the EDPS is full member. In the General Approach of the Council, the EDPS is a member without voting rights.
2232 As explained in Chapter 4 of this study.
2233 See Chapter 7, Section 8.
normally composed of Member States’ representatives, who are usually experts in the field. This is a means to ensuring respect for what Vos calls a wide definition of an institutional balance: the balance between the Union and the Member States, in addition to the balance between the institutions of the European Union.

Consequently, the second requirement of a model of a European DPA deciding in individual cases is that the full involvement of national DPAs in its operation must be guaranteed.

Towards a closer cooperation within a European DPA

The negotiations on the General Data Protection Regulation have resulted in an EDPB having features of a European DPA, because it will have certain binding powers in individual cases. To the extent the EDPB is allotted binding powers, this consequence is evident, because, where the EDPB uses these powers, the national DPAs are no longer sovereign to ensure the control of the EU rules on data protection.

Parallels exist with the granting of binding powers in other areas of EU law where European agencies are endowed with decision-making powers, thereby centralising the governance of EU law in specific areas. This centralisation happens in particular in the financial sector where agencies have been set up as a result of the financial crisis. An example is the European Banking Authority, which has direct intervention powers, including the power to take decisions that are binding upon national authorities in case of breach of EU law by a national authority. In this mechanism the national authorities are initially given the possibility to comply voluntarily with a recommendation of the European agency. The European Banking Authority also has the task to take binding decisions to settle a disagreement between two or more national authorities.

A further step in the centralisation of governance is giving supervisory powers to a European agency. EU law attributes supervisory powers to the European Securities and Markets Authority (ESMA). Where this authority establishes that a credit rating agency has

---

committed a certain infringement, it must impose a fine.\textsuperscript{2240} In this procedure there is no role for national authorities.

This further step is not included in the legislative documents on the EDPB. However, these documents allot a binding role vis-à-vis the national authorities that to a certain extent is comparable to the power of the European Banking Authority. The European Parliament is reticent concerning the grant of binding powers to the EDPB.\textsuperscript{2241} The European Parliament introduces this power as an \textit{ultimum remedium} that only becomes effective in case various previous consultations between DPAs – within and outside the framework of the EDPB – do not lead to consensus. Moreover, this binding power is presented as only binding on the DPA concerned. The Council, too, shows reticence.\textsuperscript{2242} In the contribution of the Council, the EDPB will take a decision and on that basis the DPA will take the “final decision”. These formulas suggest that decisions of the EDPB do not give rights and obligations to others than DPAs.

This suggestion is rebuttable. Where the EDPB exercises binding powers, one may assume that a decision of the EDPB can be challenged before the Court of Justice under Article 263 TFEU, which provides that a “natural or legal person may […] institute proceedings against an act addressed to that person or which is of direct and individual concern to them”. This provision must be interpreted under the \textit{Plaumann} case law. Persons are individually concerned by a decision even if they are not the addressees thereof, “if that decision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from all other persons”.\textsuperscript{2243} It is safe to say that where the EDPB will take a binding decision in individual cases, the data controllers and processors, as well as probably the data subjects, are directly affected, even though this decision is not addressed to them.\textsuperscript{2244}

Furthermore, arguably, also where the EDPB will only have advisory powers in individual cases, it will be fulfilling tasks of a DPA in ensuring control, and will have characteristics of a DPA. Advices by the EDPB will have strong persuasive power and are expected to play an important role in the subsequent enforcement by a DPA. This is the rationale behind the advice: that it is followed by DPAs and hence contributes to the uniform application of EU data protection law. A national DPA that does not follow an advice of the EDPB will be under a heavy obligation to state the reasons for its decision, and to defend this decision before a tribunal. Obviously, there is a difference with the situation of binding powers, if only because a non-binding advice cannot be the subject of proceedings before the Court of Justice. It can only be challenged indirectly in a Member State’s court where a decision is


\textsuperscript{2241} Article 58a (7) of European Parliament legislative resolution of 12 March 2014 on the proposal for a GDPR (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

\textsuperscript{2242} Article 58a (7) of Consolidated version of the General Data Protection Regulation, in Council general approach (Council document 9565/15 of 11 June 2015).


taken by a DPA, implementing the advice of the EDPB. Hence, from the perspective of legal certainty, a binding power of the EDPS is the preferred option.

Closer cooperation within a European DPA also requires that the European DPA is enabled to fulfil its task. For this reason legal personality as a EU body is relevant, as well as the availability of sufficient budget, staff and other resources, and independence in using these resources.

And the role of the Commission?

The role of the Commission in the EDPB – as was explained before in relation to the structured network – requires consideration, and even more so where the EDPB has binding powers and acts as a European DPA. The right of the Commission to participate in the activities and meetings of the EDPB without any exceptions is not in line with the requirement of independence of DPAs where this is understood as meaning the absence of “any direct or indirect external influence on the supervisory authority”, as further specified in Commission v Austria. The EDPB acting as a DPA should have the possibility to deliberate in enforcement cases without the Commission representative being present.

Procedural guarantees

Paradoxically, it would be easier to guarantee the accountability of a European DPA – especially where it has binding powers – than in the case of a structured network of DPAs.

Assuming that a European DPA qualifies as an EU body, it is part of the EU administration and for this reason subject to the same administrative requirements as other EU institutions and bodies. This means, for instance, that complaints on maladministration can be made to the European Ombudsman, that the rules on audits and fraud apply and that the European DPA is subject to the EU regulations on public access to documents and on data protection. These administrative requirements enhance the democratic accountability of the European DPA. The judicial review of its decisions is a task of the Court of Justice.

Further conditions

2245 As explained, in Article 64(4) of Commission Proposal for a GDPR, COM (2012), 11 final.
2246 Case C-518/07, Commission v Germany, EU:C:2010:125, at 19.
2247 Case C-614/10, Commission v Austria, EU:C:2012:631, at 62-64. See Chapter 7, Section 9 above.
2250 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
2251 The Legal Service of Council gives arguments why review by the CJEU complies with Article 47 Charter. Council document re Interinstitutional file 2012/0011 (COD), e.g., 18031/13 (19 Dec 2013, full version on lobbyplag.eu), at 43.
The proposed General Data Protection Regulation does not provide for any role for the EDPB in relation to EU bodies such as Europol and Eurojust, nor in relation to the information systems where the mechanism of coordinated supervision is applied. It was suggested in the ReNEUAL Model Rules on EU Administrative Procedure to give such a role to the EDPB. This suggestion is useful considering the main perspective of the EDPB, which is formulated as ensuring the consistency of the application of the proposed regulation. This perspective could also be interpreted as ensuring the consistent application of EU data protection law in general, because, as was explained above, the reform of the data protection rules is based on a comprehensive approach.

12. Cooperation between DPAs: Ensuring Independence, Effectiveness and Accountability of DPAs and the Cooperation Mechanisms, a Final Assessment and a Proposal

The layered structure of cooperation mechanisms should not compromise the independence of DPAs

Primary EU law provides that compliance with data protection rules shall be subject to control by independent DPAs. This starting point does not preclude that, where DPAs cooperate, they share the powers to ensure control within their own jurisdiction with DPAs in other jurisdictions or within an institutional mechanism for cooperation, in a composite administration. Where a cooperation mechanism has features of a European DPA, it must itself fulfil the requirements of independence as laid down in the Court of Justice’s case law.

Under Article 16(2) TFEU and Article 8(3) Charter, an individual is entitled to effective control by a DPA. As will be explained below, ‘proximity’ is not a prerequisite for legal protection under EU law. Hence, an individual has no entitlement to protection being provided by the DPA in the Member State where he or she resides. However, even where the DPA in the Member State where he or she resides is not capable of delivering effective protection, the individual must be protected, either by the DPA in another Member State or by an institutional mechanism that itself fulfils the criteria of independence under the case law of the Court of Justice.

The layered structure should contain incentives for effective protection and should not result in an incomplete – or extremely complex – system of remedies

---

2252 Research Network on EU Administrative Law, ReNEUAL Model Rules on EU Administrative Procedure, Article VI-39.
2253 In Chapter 6, Section 3.
2254 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010), 609 final.
Cooperation mechanisms are to a large extent justified by considerations of effectiveness, particularly in an internet environment, because these mechanisms should contribute to ensuring privacy and data protection by bridging the gap between principles and practice. Arguably, the contribution to the effectiveness of ensuring privacy and data protection is the main *raison d’être* for cooperation mechanisms.

Effectiveness of enforcement by DPAs requires a strong cooperation mechanism that is able to deal with the challenges in an internet environment with big data, mass surveillance and loose governance structures. *A priori*, a strong European dimension of the enforcement enhances the effectiveness, particularly the enforcement vis-à-vis big internet players. In addition, the mechanism itself should contain incentives for effective protection.

In a composite administration where multiple partners are involved in processes, the effectiveness of control requires appropriate decision-making structures, within this administration. In an internet environment prompt responses may be needed, for example in the case of a notification of a personal data breach. Consensual decision-making, with the involvement of all concerned DPAs, does not necessarily guarantee the most prompt and, hence, effective response.

Furthermore, the effective implementation by the individual DPAs of the recommendations of the cooperation mechanism should be ensured. At the same time, there should be a system for monitoring the effectiveness of the cooperation mechanism itself.

More generally, the layered structure should not result in an incomplete – or extremely complex – system of remedies, which would not only be ineffective, but would also be contrary to the right to an effective remedy in Article 47 Charter.

*Democratic accountability: the European Parliament has a role to play*

The involvement of authorities of the Member States in the control of privacy and data protection increases the legitimacy of the protection of these fundamental rights. Chapter 7 explained the advantages in terms of legitimacy, where national DPAs operate in between the Union and the Member States.

In all three models of cooperation, there is a complex relationship with the public and political accountability of DPAs before democratically elected bodies. The link with these bodies is by definition link. DPAs are not only a separate branch of government, they also have responsibilities for the protection of personal data outside the jurisdiction of the

---


Member State in which they are established. It is a part of their duty under EU law to contribute to the uniform application of EU data protection law.

The independence of DPAs limits their democratic accountability. However, the Court of Justice underlined in Commission v Germany\textsuperscript{2258} that some democratic accountability exists. The control by a DPA – albeit independent – remains linked to a democratic body. In an integrated or composite administration it is not evident at what level this link is made. Apart from national parliaments, the European Parliament also has a role to play, since the DPAs derive their tasks directly from the Treaties and duties are assigned directly by EU law.

Where DPAs take decisions in individual cases, the perspective of democratic accountability is less relevant, since the independence of the DPAs precludes accountability of DPAs for the performance of their tasks before a majoritarian body.\textsuperscript{2259} A more general allocation of decision-making responsibilities to a cooperation structure of the DPAs – instead of to individual DPAs – does not necessarily adversely affect the democratic accountability, since this type of accountability, by definition, is not focused on individual decisions, subject to judicial redress in accordance with the rule of law.

*Judicial accountability: effective redress mechanisms, not necessarily proximity*

In a composite administration, DPAs are liable before national courts, but at the same time they are not sovereign in taking decisions. DPAs should seek consensus with their peers, and, possibly, depending on the model in which they operate, they may even be obliged to execute decisions by a transnational body of peers. A precise allocation of decision-making competences is particularly important from the perspective of judicial accountability.

A further issue revealed by the negotiations on the General Data Protection Regulation relates to the legitimacy of cooperation mechanisms, from the perspective of the legal protection of the individual. The legitimacy of cooperation mechanisms requires that EU citizens have direct access to protection (judicial accountability). As far as the rights of individual data subjects are concerned, effective redress must be guaranteed before a DPA and before a court, in accordance with the requirements of Article 47 Charter, which guarantees access to justice. The system of redress must be “sufficiently coherent and clear”.\textsuperscript{2260} The requirement of a sufficiently coherent and clear system of redress plays a role in the assessment of the system of redress under the cooperation and consistency mechanisms in the proposed General Data Protection Regulation.\textsuperscript{2261}

The question arises whether EU law also requires – in addition to these general commitments – individual data subjects to have redress before a DPA within the Member State where they

---

\textsuperscript{2258} Case C-518/07, Commission v Germany, EU:C:2010:125, at 41-46, see Chapter 7, Section 9, of this study.

\textsuperscript{2259} As explained in Chapter 7.


\textsuperscript{2261} The contribution of the Council contains complicated procedures that are not necessarily coherent and clear. See, e.g., Article 54a of Council general approach (Council document 9565/15 of 11 June 2015).
reside and to have access to justice in this same Member State, directly and upon appeal against a decision of this DPA. This is the notion of ‘proximity’ that was raised during the legislative negotiations on the General Data Protection Regulation.\textsuperscript{2262} Provisions reflecting this notion can be found in EU consumer law, for instance in the provisions on jurisdiction over consumer contracts. Article 18 of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters\textsuperscript{2263} provides that consumers may always bring a case before a court in the country where they reside, also where the other party is domiciled elsewhere. Moreover, proceedings against consumers may only be brought before a court in the country of residence of the consumer.

This raises a further question: is ‘proximity’ a principle under EU law, in particular to ensure compliance with Article 47 Charter? In a case relating to agricultural parcels, the European Court of Justice did not consider it a decisive factor that the parcels concerned were far away from the competent court. However, what counts is that a “jurisdiction rule does not cause individuals procedural problems in terms, inter alia, of the duration of the proceedings, such as to render the exercise of the rights derived from European Union law excessively difficult”.\textsuperscript{2264} This is also in line with the case law on the rule of law emphasising that EU law provides for a complete system of judicial review,\textsuperscript{2265} but does not specify where this review needs to take place. For example, it is beyond doubt that direct access for individuals in the European Union to the Court of Justice itself, based in Luxembourg, is in line with EU law, even in cases where these individuals reside in remote areas of the Union, far away from the Grand Duchy.

In short, ‘proximity’ is not a prerequisite for legal protection under EU law. What counts is the effectiveness of redress mechanisms. However, although access to redress mechanisms close to the citizens may not be required from the perspective of judicial accountability, it may enhance the (democratic) legitimacy of EU action, when there are remedies “as closely as possible to the citizen”\textsuperscript{2266}

\textit{The final assessment and a proposal}

Administrative networks – in various constellations – play an increasingly strong role in the implementation of EU law and policy, which is, in principle, a duty of the governments of the Member States. The cooperation between DPAs fits within this trend. The fact that the DPAs have a special status as a result of their mandate based directly on primary EU law – Article 16(2) TFEU and Article 8(3) Charter – makes the need for cooperation even more important.

\textsuperscript{2262} In particular in the Council, see Chapter 7, Section 12.
\textsuperscript{2264} Case C-93/12, \textit{Agrokonsulting-04}, EU:C:2013:432, at 52 and 61.
\textsuperscript{2266} Wording taken from Article 1 TEU.
The control of the compliance with data protection rules is not centralised at the EU level. Although considerations of effectiveness plead in favour of a uniform and harmonised approach of the control, this does not mean that centralisation of the control would be the preferred option, at least not in the immediate future. Centralisation of the control is also not favoured in any of the contributions of the EU institutions in the legislative process concerning the General Data Protection Regulation.

The importance for the individual to have redress in the Member State of residence plays a role, and also the preference to leave responsibility with the Member States, in line with the main structure of the European Union, which is based on decentralised implementation. This is even more relevant, in view of the subject matter: the protection of fundamental rights, which is a core task of governments.2267

From these perspectives, the study presents these three models as part of a layered structure for an independent, effective and accountable control on EU data protection. This structure consists of three models: cooperation of DPAs, consisting of horizontal cooperation, a structured network and a European DPA. This layered structure must guarantee that the two objectives of cooperation of DPAs are satisfied: the protection of individuals vis-à-vis entities established outside the national territory, as well as the uniform interpretation of EU data protection law. The EDPB, as proposed in the General Data Protection Regulation, could function both as a structured network and as a European DPA.

The added value of this layered structure is, in the first place, to clearly define where cases could be handled in the first layer, horizontal cooperation. If a case concerns data subjects in a large number of Member States, normally, horizontal cooperation will not be sufficient. In the second place, this structure allows making a distinction in the activities of the EDPB in a consistent manner, reconciling legitimacy and effectiveness.

The EDPB could act as structured network, where it fulfils an advisory role, giving guidance to DPAs, as well as to the EU institutions. This role would be subject to lower standards of independence of the EDPB, with a lower level of procedural guarantees and lower requirements on the participation by the DPAs, and could include the participation of the European Commission, in particular to ensure the harmonised application of the rules under Article 16 TFEU.

The standards for independence increase in proportion to the extent the EDPB acts as a European DPA, with decision-making power. The EDPB should be bound by the same standards of independence as national DPAs and procedural guarantees are required, comparable to the ReNEUAL Model Rules on EU Administrative Procedure.2268 The law should specify the participation by the DPAs, and the European Commission should not participate in the decision-making. Moreover, the EDPB, acting as a DPA, should have the

2267 See, mostly, Chapter 4.
possibility to deliberate in enforcement cases without the Commission representative being present. The system of redress must be sufficiently coherent and clear. Proximity, in the sense that an individual is entitled to redress in the Member State where he or she resides, is not a prerequisite for legal protection under EU law.

This proposal should guarantee that the two objectives of cooperation of DPAs are satisfied: the protection of individuals vis-à-vis entities established outside the national territory, as well as the uniform interpretation of EU data protection law. Unfortunately, in the negotiations on the General Data Protection Regulation, the emphasis is mainly on the first objective, by positioning the consistency mechanism more as a structure for conflict resolution than as a means for ensuring the uniform application of the law in the European Union.

13. Conclusions

Under EU law, DPAs have a hybrid position operating in between the Union and the Member States. They are part of an integrated or composite administration, based on a horizontal collaboration between administrative organs in a non-hierarchical manner. This integrated or composite administration is the result of a trend where the separation of duties between the European Union and the Member States is becoming less clear and is complemented by forms of administrative cooperation where duties are shared, not separated.

The mandate of DPAs comprises the obligation to contribute to a harmonised and effective level of data protection within the wider territory of the European Union. This is particularly important in an internet environment, where dealing with cross-border effects is an inherent element of the protection that must be given. Moreover, this obligation for DPAs is the consequence of the recognition that the European Union is the appropriate platform for dealing with internet privacy and data protection. In the light of these circumstances, enforcement has also become an EU concern.

DPAs should contribute to the control of data protection outside of the territory of their constituent Member State, mutually cooperating with their peers across the border. The proposed General Data Protection Regulation intends to strengthen the institutional cooperation, with the establishment of the EDPB. (Section 2)

The duty for ensuring control in a cross-border context and for mutual cooperation follows from the system of EU law. There is a parallel with the remedies under national law, ensuring legal protection against breaches of EU law. Mutual enforcement cooperation consists of exchanging information, effectively assisting in supervision and – after the entry into force of the GDPR – the carrying out of joint investigative tasks, joint enforcement measures and other joint operations. (Section 3)

Presently, the Article 29 Working Party is the core mechanism for institutional cooperation between DPAs, with as its primary task contributing to the uniform application of the
national rules adopted pursuant to Directive 95/46. The further task of contributing to a harmonised and effective level of data protection within the wider territory of the European Union is also mainly attributed to the Working Party. The contribution of the Working Party consists of giving non-binding guidance, indirectly influencing the supervision by the DPAs, but in a significant way. The Joint Supervisory Bodies of Europol and Eurojust are at present the only institutional cooperation mechanisms with enforcement powers. (Section 4)

The GDPR introduces two novelties. The first novelty is a one-stop shop mechanism with a lead supervisory authority cooperating with its peers in cases where DPAs in more than one Member State are concerned. The involvement of all DPAs must ensure that in any single case only one decision is taken and, at the same time, prevent that multinational companies have to deal with divergent enforcement decisions and ensure that they have a sole interlocutor. Under the consistency mechanism, the second novelty, the EDPB, as the successor of the Article 29 Working Party, will have a formal role in enforcement. For the Commission, this mechanism serves as a conflict-solving mechanism between concerned DPAs and also as a mechanism to ensure the correct and consistent application of the regulation within the wider territory of the European Union. This study concurs with the wide approach of the Commission. (Section 5)

The study compares the DPA cooperation with the supervisory network in the electronic communications sector, which consists of a network of national authorities and of BEREC. This comparison shows how consistency can be organised. The history of BEREC is also relevant for the purpose of comparison, because it bears witness to the reticence that exists against centralisation of enforcement. In electronic communications, BEREC has an authoritative status, because national authorities are obliged to take the utmost account of BEREC’s positions. The Commission took the mechanism of governance in electronic communications as inspiration for the consistency mechanism in its GDPR proposal. (Section 6)

Administrative cooperation under EU law is a matter of common interest. Rules on administrative procedure should ensure the effective discharge of public duties and the protection of individuals’ rights. Arguably, in light of the fundamental right of an individual to a good administration, as laid down in Article 41 Charter, the DPA cooperation should meet both objectives.

Procedural guarantees – as included in the ReNEUAL Model Rules on EU Administrative Procedure – could deal with the disadvantages of fragmentation of administrative law in the European Union, also in the area of data protection. The principle of sincere cooperation has an additional dimension in a composite administration where cooperation between the various actors and levels is a condition for success. The principle of sincere cooperation extends to cooperation with authorities in related policy areas. Where DPAs cooperate with actors outside government, the latter should respect principles of good governance, but Article 4(3) TEU does not apply to non-governmental stakeholders. (Section 7)
This study distinguishes three models of cooperation: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models are examples of the integrated or composite EU administration where competences are not divided but shared. The main differences between these three models relate to the nature of coordination. (Section 8)

Horizontal cooperation is characterised by the sharing of responsibilities, a common interest, good faith and good administration in the absence of hierarchy. Horizontal cooperation is not limited to two DPAs, but relates to all concerned DPAs. Where goods or services are offered on the internet, this cooperation can involve the DPAs of all 28 Member States. Hence, horizontal cooperation is not always effective. Horizontal DPA cooperation requires specifying procedural guarantees, in order to facilitate the cooperation and to further specify the guarantees at EU level. (Section 9)

The cooperation of DPAs as expert bodies should also enhance the uniform application of EU data protection law within the European Union. The cooperation mechanisms give effect to the task of DPAs to contribute to the control in the entire European Union, but they are also an expression of democratic legitimacy, involving decision-making close to the citizen. Under the GDPR, the structured network of DPAs will be reinforced by the establishment of the EDPB. The EDPB acts as structured network, where it fulfils an advisory role giving guidance to DPAs as well as to the EU institutions.

The increased duties and powers of the network in the EDPB imply that stricter requirements for composition and decision-making structures must be complied with. The composition of the EDPB by senior representatives of DPAs, as well as consensual decision-making procedures, enhance the legitimacy of the EDPB. A close relationship between the Commission and the EDPB as a structured network is desirable from the perspective of consistency, but direct influence on the decision-making process should be avoided. A structured network requires procedural rules. (Section 10)

It is expected that the EDPB will have – binding – powers to ensure the compliance with data protection rules. When the EDPB exercises these powers, it becomes a DPA and it should fulfil the conditions of independence as laid down in the Court of Justice’s case law. Procedural guarantees are required, comparable to the ReNEUAL Model Rules on EU Administrative Procedure. The law should specify the participation by the DPAs, and the European Commission should not participate in the decision-making. The system of redress must be sufficiently coherent and clear. Proximity, in the sense that an individual is entitled to redress in the Member State where he or she resides, is not a prerequisite for legal protection under EU law. Where the EDPB exercises binding powers, one may assume that a decision of the EDPB can be challenged before the Court of Justice, under Article 263 TFEU. (Section 11)

DPAs operating in multiple jurisdictions create a further challenge for reconciling their independence, effectiveness and accountability. The layered structure of DPA cooperation should not compromise the independence of DPAs. Increasing the duties and powers of the EDPB sets higher standards for its independence, including a higher level of procedural guarantees and stronger requirements on the participation by the DPAs. Effectiveness of enforcement by DPAs requires a strong cooperation mechanism that is able to deal with the challenges in an internet environment with big data, mass surveillance and loose governance structures. For example, the effective implementation by the individual DPAs of the recommendations of the cooperation mechanism should be ensured. At the same time, there should be a system for monitoring the effectiveness of the cooperation mechanism itself, so as to avoid that DPA cooperation results in an incomplete – or extremely complex – system of remedies, in breach of Article 47 Charter. A degree of accountability vis-à-vis the political institutions of the Member States is a priori required for DPA cooperation to be successful and legitimate. Where the EDPB – which is largely composed of national DPAs – acts as a European DPA, the involvement from the European Parliament as the body ensuring some degree of political accountability is obvious. However, the EDPB should also trigger involvement from national parliaments. (Section 12)

The study presents these three models – horizontal cooperation, a structured network and a European DPA – as part of a layered structure for an independent, effective and accountable control on EU data protection. This layered structure should guarantee that the two objectives of cooperation of DPAs are achieved: the protection of individuals vis-à-vis entities established outside the national territory, as well as the uniform interpretation of EU data protection law. The EDPB, as proposed in the GDPR, could function both as a structured network and as a European DPA.

The added value of this layered structure is, in the first place, to clearly define where cases could be handled in the first layer, horizontal cooperation. If a case concerns data subjects in a large number of Member States, normally, horizontal cooperation would not be sufficient. In the second place, this structure allows making a distinction in the activities of the EDPB in a consistent manner, reconciling legitimacy and effectiveness.

The EDPB could act as a structured network, where it fulfils an advisory role, giving guidance to DPAs, as well as to the EU institutions. This role would be subject to lower standards of independence of the EDPB, with a lower level of procedural guarantees and lower requirements on the participation by the DPAs, and could include the participation of the European Commission, in particular to ensure the harmonised application of the rules under Article 16 TFEU.

At present, the control of the compliance of data protection rules is not centralised at the EU level. Although considerations of effectiveness plead in favour of a uniform and harmonised approach of the control, this does not mean that centralisation of the control would be the preferred option, at least not in the immediate future. Centralisation of the control is also not
favoured in any of the contributions of the EU institutions in the legislative process concerning the GDPR.

It is recommended that the layered structure be elaborated as a structure for a better governance of control of data privacy and data protection in the European Union. The layered model is not meant to centralise essential parts of the decision-making by DPAs to the European level, but to ensure that, where the European level is involved in the control on data protection, appropriate standards are in place.
Chapter 9. Understanding the EU Mandate under Article 16 TFEU in the External Domain: Towards a Mix of Unilateral, Bilateral and Multilateral Strategies

1. Introduction

In an internet environment any processing of personal data potentially takes on a global dimension. Personal data processed in the open parts of the internet are in principle ubiquitously accessible all over the globe, the big cloud providers storing huge amounts of personal data are global players and the geographical location where data are stored has become irrelevant because data are present in multiple jurisdictions at the same time.\textsuperscript{2270}

This chapter analyses the mandate of the European Union under Article 16 TFEU in the external domain, a component of the research question with relevance for all actors referred to in Article 16 TFEU: “what does and should the European Union do to make Article 16 TFEU work in the external domain?” This analysis includes the following subjects:

a. the general design of EU data protection on a global the internet;

b. the institutional component and the DPAs in the external domain;

c. the relationship with the most relevant third countries and international organisations;

d. the relationship between EU law and international law;

e. jurisdictional issues;

f. three strategies for the European Union in the international domain: unilateral, bilateral and multilateral, with an emphasis on the unilateral approach;

g. the meaning of the strategies for the actors referred to in Article 16 TFEU.

The first objective of this chapter is to understand the pluralist legal context in which the European Union operates with competing jurisdictional claims of third countries and international organisations. The second objective is to develop a strategy for the action in the external domain based on a mix of unilateral, bilateral and multilateral strategies.

The global nature of the internet and the extraterritorial effect of EU action require that in the external domain solutions are found for two types of issues: conflicting jurisdictional claims and divergences in substantive law.

Section 2 describes the general scheme of EU data protection in relation to third countries and international organisations. Section 3 focuses on the institutional component of EU privacy and data protection, which is embodied in the DPAs and the cooperation mechanisms. Section 4 discusses some main elements of the protection of data privacy in the

\textsuperscript{2270} Further read: Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing 2013, at 27 (incl. footnotes mentioned there).
The United States is the prime example of a jurisdiction in which different views are held on questions concerning conflicting jurisdictional claims and that diverges from the European Union on matters of substantive law. Sections 5 and 6 deal with the international organisations concerned. Article 220(1) TFEU specifies a few international organisations with which the European Union has to establish appropriate forms of cooperation. In general, these organisations are also active in the governance of the area of data protection and, consequently, are specifically addressed in this study: the United Nations and, where relevant, its specialised agencies, and the Organisation for Economic Co-operation and Development (“OECD”) are discussed in Section 5, whereas the Council of Europe is addressed in Section 6.

Section 7 of this chapter introduces the pluralist context in which the European Union operates in the external domain. This obviously encompasses the relations with third countries and international organisations. In addition, the section discusses the internal division of powers in the European Union in relation to external action. Sections 8-10 address different issues that are at play when establishing jurisdiction on the internet. Section 8 first establishes the primacy of international law and its relation to EU law, while Section 9 focuses primarily on public international law and Section 10 discusses the link between internet jurisdiction and the protection of individuals.

To conclude the chapter, the last few sections discuss the EU action on the international scene. Section 11 introduces the three strategies the European Union may take in the external domain. The strategies themselves – unilateral, bilateral and multilateral – are explained in Sections 12-14. The Sections 15-17 contain a synthesis: what does this all mean for the Court of Justice, the EU legislator and the Data Protection Authorities? Section 18 presents the conclusions of this chapter.

2. A General Design of EU Data Protection on a Global Internet and the Relationship with Third Countries and International Organisations

On the internet, every activity of a data controller or processor located outside the European Union may have an impact on individuals inside the EU territory. The internet is a borderless zone, despite trends towards a fragmentation of the internet that could result in the internet being separated into regional fractions. Vice versa and for the same reason, every activity of a data controller or processor inside the European Union may have extraterritorial effect, if only because personal data within the Union are in principle accessible from outside the

---

2271 For reasons explained in Chapter 1, Data privacy - not data protection - is the term used in the United States.
2272 Article 220(1) TFEU also mentions the Organisation for Security and Cooperation in Europe (OSCE), but that organisation has no specific relevance for this study.
2273 As explained in Chapter 3, Section 4, On the relation between fragmentation of the internet and data protection, see Internet Balkanization gathers pace: is privacy the real driver?, Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svitessson, and Orla Lynskey, International Data Privacy Law, 2015, Vol. 5, No. 1.
Union, and also because personal data of EU residents are transferred outside the Union. Finally, due to the networked structure of the internet personal data are at the same time available in various jurisdictions.

EU law determines the territorial boundaries of the Union’s jurisdiction. In the physical world, these boundaries are determined by the physical borders of the European Union and the Member States. In the information society this is more complicated. Exercise of EU competence on the internet affects legitimate claims to sovereignty by third countries, and also instruments of international law, be it in the areas of privacy and data protection or in other related areas.\textsuperscript{2274} This is the external effect of the exercise of internal powers of the European Union.

The borderless nature of the internet means that – as a rule – any intervention by the European Union with the purpose of protecting privacy and data protection on the internet has extraterritorial effects. Moreover, giving extraterritorial effect to EU data protection law is an explicit objective of the EU legislator, which is justified by the simple reason that effective protection of Europeans would not be guaranteed if the protection were to end when personal data cross EU borders. This connects to what was discussed earlier in this study: privacy and data protection are essential in a democratic society, for individuals as well as society itself.\textsuperscript{2275} We also mentioned the claim of the universality of EU fundamental rights,\textsuperscript{2276} resulting in the general ambition of the European Union to promote its essential values, also in the wider world.

Directive 95/46 on data protection acknowledges that extraterritorial protection must be given to individuals residing in the European Union who deal with data controllers outside the EU territory. Article 4(1)(c) of the directive extends the scope of application of the directive to data controllers outside the EU territory that make use makes use of equipment, automated or otherwise, situated on the territory of a Member State. This rule on extraterritorial protection will be significantly broadened in the General Data Protection Regulation, which also will include the offering of goods or services to individuals in the European Union and the monitoring of their behaviour.\textsuperscript{2277}

The extraterritorial effect of acts of a data controller or processor inside the European Union is recognised in Article 25 of Directive 95/46 on the transfer of personal data to third countries giving explicit extraterritorial effect to the directive. Article 25 of the directive must not only ensure a high level of data protection, but it also acknowledges the necessity of international trade, which includes personal data.\textsuperscript{2278} This provision was interpreted by the

\textsuperscript{2274} As illustration, just one example: the Cybercrime Convention (Council of Europe, Committee of Ministers (2001), Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001, entered into force on 1 July 2004) is often related to the right to data protection: see: Handbook on European data protection law, 2nd edition, Fundamental Rights Agency, at 148.
\textsuperscript{2275} This is the conclusion of Chapter 2.
\textsuperscript{2276} As expressed in the preamble and in Article 21 of the TEU. See Chapter 2, Section 2 of this study.
\textsuperscript{2277} Article 3(2) of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
\textsuperscript{2278} Recital 56 of Directive 95/46, as confirmed by the CJEU in Case C-362/14, Schrems, EU:C:2015:650, at 48.
European Court of Justice in an early ruling on EU data protection, *Lindqvist*.

The Court limited the notion of transfer of personal data under Article 25 of Directive 95/46 and excluded that all posting of personal data on the internet was to be considered as a transfer of data.

The external dimension is even more predominant in view of the fact that data are ubiquitously available and not only present in one jurisdiction. This reality is not reflected in current EU data protection law and also not covered by the General Data Protection Regulation, which continues to take the transfer of personal data to a third country as the point of reference for EU jurisdiction.

*Externally, the EU operates in a pluralist legal context*

The division of competences between the European Union and the Member States was analysed in Chapter 4, which describes a pluralist legal context. Externally, the European Union also operates in a pluralist legal context, which is determined by relationships with third countries, as well as with international organisations.

The horizontal relationship between the European Union and the jurisdictions of third countries is one of the main factors complicating effective internet regulation. There is an inherent coincidence of EU law with other legal systems. Third countries, too, have legitimate claims to regulating personal data on the internet, including data of Europeans. These claims are based on considerations of privacy and data protection and also on other public interests. The claims coincide or even collide with those of the European Union, and hence contribute to positive conflicts of jurisdiction.

Another complicating factor is the vertical relationship between the European Union and international organisations that are active in the area of privacy and data protection, and that are based on international law to which the European Union is subject. EU law may coincide with legal and other instruments of international organisations that are applicable to the EU Member States and sometimes to the EU level as well.

The relationship between the European Union and these external actors is determined by international law, but is also influenced by EU law itself. The interaction between international law and EU law further amounts to a pluralist legal context, in addition to the internal division of competences.

### 3. The Institutional Component of EU Privacy and Data Protection in the External Domain, focusing on the DPAs and their Cooperation

---


All actors who contribute to the fulfilling of the mandate of the European Union under Article 16 TFEU play a role in the external domain. The Court of Justice as the highest EU court ensures that the right to data protection itself is protected. Chapter 5 discussed the role of the Court, which in its capacity of a constitutional court focuses on ensuring the protection of the fundamental rights, yet also ensures that the commitment to integration is delivered and that it acts as an umpire where conflicts of competences occur. These roles of the Court all have external components in an internet environment.

The EU legislator assumes its role in the external domain in two manners. The internal EU legislation contains provisions with the aim of giving extraterritorial effect to the internal legislation, with Articles 4(1)(c) and 25 of Directive 95/46 on data protection as the examples. In addition, the EU legislator has external competences, for instance to conclude agreements under Article 16(2) TFEU, first sentence, read in connection with Article 216 TFEU. Article 216 TFEU can be seen as the consolidation in the Treaties of the doctrine of implied external powers, developed by the Court. The procedure for concluding international agreements is laid down in Article 218 TFEU, and ensures the involvement of the Council, the Commission and the European Parliament. Obviously, these roles of the EU legislator are highly relevant in an internet environment.

From an institutional perspective, the Court and the EU legislator do not fulfil a specific role in the area of privacy and data protection. In contrast, the mandate of the DPAs of the cooperation mechanisms of the DPAs does raise a specific institutional issue. DPAs have been qualified in this study as new branches of government, cooperating in a composite or integrated administration. Their mandate includes ensuring control in cases with an external dimension, for instance because the data controller or the personal data are located outside the European Union; the advisory role of the DPAs, too, has external aspects. The institutional issue referred to concerns the representation of the European Union in the international context by DPAs or by cooperation mechanisms of the DPAs.

A specific issue: the representation of the EU in the international context and the role of cooperating DPAs

The external representation of the Union is a complex matter, as was illustrated by the famous quote of the former US Secretary of State Henry Kissinger: “Who do I call if I want to call Europe?” Chapter 7 qualified the DPAs as a new branch of government, which might mean that the DPAs also have a position in the external representation of the Union, within the boundaries of their responsibility. The understanding of this provision provokes two related questions. What are the boundaries of their responsibility within the external domain and who should be the face of the European Union in this area? Is this the EDPS as

---

the European body for data protection or is this the Chair of the Article 29 Working Party, as the representative of all European DPAs?\(^{2284}\)

This study will only discuss the first question, on the boundaries of the responsibility. In general, as part of their mandate the DPAs must interact with data protection regulators in third countries and, where relevant, with international organisations.\(^{2285}\) However, they should remain within the boundaries of their responsibilities and should not act in the domain of other EU bodies. In the external domain, too, they are bound by the principle of sincere cooperation laid down in Article 4(3) TEU, which is considered to be a reflection of federal good faith.\(^{2286}\)

The position in the external domain has been specified for EU agencies in Point 25 of the Joint Statement and Common Approach of the European Parliament, the Council of the European Union and the European Commission on Decentralised Agencies.\(^{2287}\) Although the independence of DPAs distinguishes them from EU agencies,\(^{2288}\) the Joint Statement and Common Approach contains elements with relevance for the independent DPAs.\(^{2289}\) In the first place, the statement mentions that the agencies should operate within their mandate and within the existing institutional framework and that they should not be seen as representing the Union. In the second place they should not commit the Union to international obligations. In the third place, they should exchange information on their activities with the Commission and relevant EU delegations in order to ensure the consistency of EU policy.

For DPAs, these elements reflect a paradox between, on the one hand, the independence of DPAs, which should allow them to take position without having to consult other institutions or bodies, and, on the other hand, the need for unity of the European Union in its external relations.

The solution of this paradox should probably be found in the principle of sincere cooperation as a reflection of federal good faith. This requires the DPAs to inform the institutions where positions are taken and take account of the feedback given by the institutions in view of ensuring the consistency of EU policy. It also requires them being transparent to the partners in third countries and international organisations. The principle of sincere cooperation also commits the EU institutions to involve the DPAs where they take positions in the external domain on policies concerning privacy and data protection. This commitment may, by way of

\(^{2284}\) The second question is mainly mentioned as an illustration of the relevance of the quote of Kissinger, but the answer exceeds the scope of this legal study.

\(^{2285}\) As explained for EU agencies in the contribution of Ott, Vos and Coman-Kund in EU Agencies in between Institutions and Member States, Edited by: Michelle Everson, Cosimo Monda, Ellen Vos, January 2014, ISBN 9041128433, Chapter 5.

\(^{2286}\) Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010, at 7-045. This was explained in Chapter 8 for the internal EU context.


\(^{2288}\) As explained in Chapter 7.

\(^{2289}\) Other elements of Point 25 are not mentioned because they are not compatible with the independence of DPAs. However they serve as an inspirations for possible rules on enforcement cooperation with authorities in third countries and with international organisations.
example, require the Commission to involve the DPAs in negotiations on international agreements conducted with third countries in this area according to the procedure of Article 218 TFEU.

Another requirement is that agencies should not commit the Union to international obligations. It is evident that DPAs cannot conclude agreements with third countries and international organisations, since that would be incompatible with the competences laid down in Article 218 TFEU, which reflects the institutional balance between the European Parliament, the Council and the Commission. However, DPAs do conclude various forms of arrangements with authorities of third countries, such as memoranda of understanding (MOUs). Arguably, where these arrangements deal with cooperation in enforcement they are an element of ensuring control and do not prejudice the consistency of EU policy. In contrast, where arrangements are concluded on policies in the area of privacy and data protection this could affect the consistency of EU policy. The boundary is not clear.

4. The EU and Third Countries, particularly the US: A Difference in Approach

Legitimate claims of jurisdiction by third countries may coincide or even collide with EU jurisdiction on the internet. This study focuses, as far as claims of third countries are concerned, on the United States. The US has a strong position, since the most dominant internet companies have their main establishment in the US. These are precisely the companies that process large amounts of personal data of residents of the European Union. Furthermore, the US government has a leading position in IT knowledge and, finally, it has a leading role in protecting global physical security in the world as a military power, which, for instance, also extends to the fight against terrorism.

In the area of privacy and data protection, the diverging jurisdictional claims of the EU and the US are the subject of continuous political and legal debate, for instance as a consequence

---

2290 Included in in Point 25 of the Joint Statement and Common Approach of the European Parliament, the Council of the EU and the European Commission on Decentralised Agencies.
2292 As was explained in Chapter 1, Section 5.
2293 See for an illustration of this new economy dominated by the US companies, more in particular by companies in California, Manuel Castells, The Rise of the Network Society, Volume I: The Information Age: Economy, Society and Culture, 2nd edition (2010), Chapter 2.
2295 An example is the rationale behind the Terrorist Finance Tracking Program, which lead to an agreement between the EU and the US which according to its recitals recognises that "the United States Department of the Treasury’s (US. Treasury Department) Terrorist Finance Tracking Program (TFTP) has been instrumental in identifying and capturing terrorists and their financiers and has generated many leads that have been disseminated for counter terrorism purposes to competent authorities around the world, with particular value for European Union Member States"; and therefore allows transfers of personal data of Europeans to the relevant US authorities, See Agreement in OJ L 195/3.
of the differences between the legal systems on privacy an data protection. Bygrave calls this the transatlantic data privacy divide.2296

As a first consideration, the substantial elements of protection are largely the same in the EU and the US. Both systems evolved in the 1970s as a response to technological developments and – generally speaking – share the same basic principles, as both jurisdictions subscribe to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.2297 As Vladeck underlines, the EU and the US share the same aspirational goals.2298 However, there are differences. US law, for instance, does not distinguish between the value of privacy, the subject matter of Article 7 Charter, and data protection, as a system of checks and balances for the processing of personal data, included in Article 8 Charter.2299

As a second consideration, there is a systemic difference. EU law provides a comprehensive system of protection, under Article 16 TFEU and comprehensiveness is the ambition of the legislative reform in the European Union.2300 In the US there is a split between the protection in the public and the private sector. The US Privacy Act of 19742301 gives protection to individuals against data processing by the federal government and general constitutional protection – for instance under the Fourth Amendment2302 – protects the individual against the government. In the private sector, privacy and data protection are elements of consumer protection, which includes a large number of sector-specific federal and state laws.2303

As a third consideration, there is a difference in enforcement. In the US there are no independent data protection authorities, similar to the DPAs referred to in Article 16(2) TFEU and Article 8(3) Charter, although the Federal Trade Commission (“FTC”) comes close, within the areas of its competence. The FTC is not competent for the public sector for instance.

A fourth – to a certain extent controversial – consideration relates to the claims to jurisdiction on the internet on both sides of the Atlantic. An element of US law relating to privacy protection is a limitation of its scope ratione personae, in that it not always extends to

---


2297 C(2013)79, published on website OECD.

2298 David C. Vladeck, A U.S. Perspective on Narrowing the U.S.-EU Privacy Divide, in “Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime, Artemi Rallo Lombarte, Rosario García Mahamut (eds), Tirant lo Blanch, 2015.

2299 On the distinction under EU law, see Chapter 2. On the transatlantic differences, see also Chapter 6, Section 12, e.g., in relation to limitations on data collection.


2302 See Chapter 5, Section 11.

2303 See Chapter 6, Section 12.
foreigners. The US Privacy Act does not protect EU citizens, unless they have permanent residence in the US. The ruling of the US Supreme Court in *United States v Verdugo-Urquidez* excluded foreigners from the scope of the Fourth Amendment.

The wide jurisdiction claimed by the European Union in the various provisions of Directive 95/46 and confirmed by the EU Court of Justice in *Google Spain and Google Inc.* is hence not in line with the jurisdictional approach of the United States. Thus, the EU claim provoked an intensive involvement of the US government in the legislative process on the General Data Protection Regulation. This US involvement was caused not so much by the strong protection for EU citizens, but by the wide jurisdictional claim of the European Union.

An important element of this controversy is a difference in approach between the EU and the US. The approach of the US – at least in relation to consumer privacy – does not aim at giving wide territorial scope to US law, but at increasing interoperability in privacy laws by pursuing mutual recognition. It is illustrative that the US government bases mutual recognition not only on common values surrounding privacy and personal data protection, but also on effective enforcement and mechanisms for companies to demonstrate accountability. The 2012 White House Paper issued by the Obama administration explains this.

This emphasis on mutual recognition contrasts with the nature of privacy and data protection as fundamental rights under EU law, preventing the mutual recognition of substantive principles of EU law in this area if the standards in a third country do not comply with the Charter.

The background: the US and the fundamental rights protection of EU residents

---

2306 Particularly, Articles 4 and 25 of the directive.
2307 Case C-131/12, *Google Spain and Google Inc.*, EU:C:2014:317
2308 Bygrave reports, e.g., the threat of a trade war, if certain rights, such as the right to be forgotten, would not be watered down, Lee A. Bygrave, Data Privacy Law, An International Perspective, Oxford University Press 2014, Chapter 7.
2309 Further read: White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012.
2310 White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012, at 31. The paper also mentions codes of conduct and enforcement cooperation, less relevant here. See on this also, Christopher Kuner, The European Union and the Search for an International Data Protection Framework, Groningen Journal of International Law, volume 2 number 2, pp. 55-71, 2014.
2311 White House paper, Consumer data privacy in a networked world, a framework for protecting privacy and promoting innovation in the global digital economy, February 2012.
There is a connection between the explanations in the White House Paper – dealing with consumer privacy – and other manifestations of the scope of application of US law in privacy and data protection. The Fourth Amendment protects the people in the US. Moreover, it is claimed that the right to privacy as protected by the US constitution does not apply to foreign surveillance. This was an issue in relation to the Snowden revelations in the US itself, because the NSA included US persons in its monitoring activities. These persons are entitled to claim protection under the US Constitution, whereas foreigners do not have such claim.

Milanovic also claims that the limitation of the scope of the right to privacy in the ICCPR, a convention applicable to the US, to the territory of the state is the result of the position of the US government. In comparison, Article 1 ECHR has a wider territorial scope. The European Convention on Human Rights lays down that the contracting parties shall secure the fundamental rights to everyone within their jurisdiction. This difference in scope suggests that the difference of approach in jurisdiction between the US and Europe has a longstanding background.

Furthermore, various instruments under US law limit the access of non-US citizens to judicial remedies. The restricted application of significant US privacy rules to foreign citizens is a recurring theme in the discussions between the EU and the US on data protection, for instance in the negotiations on the EU-US Data Protection and Privacy Agreement for law enforcement (known as “Umbrella agreement”). This is why in March 2015 a bill was introduced in Congress extending the protection of the US Privacy Act to EU citizens, in a couple of respects.

Complexities of dealing with other third countries that have different values

This study refers to the main elements of privacy and data protection in the law of the United States, with the aim of putting the protection under EU law into a wider perspective and in order to set the scene for external action. They are meant as illustrations of challenges due to differences in legal systems and in values, in view of the fact that positive conflicts of law are a phenomenon inherent to the internet.

This study shows that these differences are difficult to overcome with countries with shared democratic values. The US is the significant, but not the only example. These differences are likely to become even more complex where the EU must deal with countries with different

---


2314 The example of the US Privacy Act of 1974 was mentioned in Chapter 6.

2315 See Conclusion of AG Bot in Case C-362/14, Schrems, EU:C:2015:650, at 213.

2316 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.

values, like some of the emerging economies. The fact that, for instance, the BRICS countries\textsuperscript{2318} are gaining more economic power makes it even more important to find solutions in relation to the external dimension of Article 16 TFEU.

5. Two of the Most Relevant International Organisations: The United Nations do Not play a Prominent Role and the OECD underlines the Free Flow of Information

The European Union is not the only international organisation that plays a role in protecting privacy and data protection on the internet. Privacy and data protection are internationally recognised concerns\textsuperscript{2319} and individuals outside the European Union, too, are entitled to protection.

This study focuses on the United Nations, the OECD and the Council of Europe as international organisations that are all to some extent involved in privacy and data protection.\textsuperscript{2320} The European Union as an organisation \textit{sui generis} interacts with these organisations.

This section does not give an overview of the involvement of these organisations in privacy and data protection, but just sets the scene for the purpose of a better understanding of the external aspects of the role of the European Union under Article 16 TFEU. Where the European Union envisages a unilateral strategy, the United Nations, the OECD and the Council of Europe are the main international organisations whose positions must be considered, when developing the strategy. Where the European Union envisages a (bilateral or) multilateral strategy, these are the logical partners. The positions of these organisations in privacy and data protection are relevant for EU action, for substantive as well as for jurisdictional reasons.

To be complete, there are also international organisations that are active in this area in other regions of the world, without direct ties with the European Union or the Member States.\textsuperscript{2321} A good example is the APEC (Asia-Pacific Economic Cooperation), which has developed (non-binding) instruments for data flows within the APEC Privacy Framework.\textsuperscript{2322}

The United Nations: should they play a more prominent role?

\textsuperscript{2318} BRICS is the acronym for five major emerging national economies: Brazil, Russia, India, China, and South Africa (source: https://en.wikipedia.org/wiki/BRICS). The study does not claim that privacy and data protection are not taken serious in any of these countries.

\textsuperscript{2319} See Chapter 2, at various places, including references to Article 12 of the Universal Declaration of Human Rights and Article 17 ICCPR.

\textsuperscript{2320} As was explained in Chapter 1, Section 5 of this study.

\textsuperscript{2321} For an overview: Transborder Data Flows and Data Privacy Law, Christopher Kuner, 2013.

\textsuperscript{2322} http://www.apec.org/Groups/Committee-on-Trade-and-investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.
In particular after the Second World War, partly as a reaction to the nationalism that lead to this war, the importance of governance by international organisations significantly increased. This development was based on the view that the way a state treats its citizens is a matter of international concern.\textsuperscript{2323} This resulted in the Universal Declaration of Human Rights (1948). Article 12 thereof proclaims the protection against interference with privacy (and family, home, correspondence, honour and reputation) to be a basic human right. In 1966, the General Assembly of the United Nations adopted the International Covenant on Civil and Political Rights ("ICCPR"), including Article 17 with largely the same substantive content as Article 12 of the Universal Declaration of Human Rights.

Some scholars embrace this development from the perspective of a cosmopolitan view or even a cosmopolitan ideal.\textsuperscript{2324} In this ideal, the individual is put at the forefront and all individuals in the world have certain universal claims. An individual is primarily a citizen of the world and from this status he derives rights and obligations. Diogenes is said to be at the basis of this ideal, when he declared: "I am a citizen of the world".\textsuperscript{2325}

The existence of a citizen of the world can also be seen as giving legitimacy to a global international organisation representing his interests and protecting his rights, such as the United Nations. There are good arguments against a cosmopolitan approach – such as the absence of democratic legitimacy and scepticism regarding the universality of fundamental rights – but many arguments defending internet freedom are based on the idea that world citizens exist and that the internet serves as an instrument to connect citizens, protecting them against arbitrary behaviour of (national) governments.\textsuperscript{2326}

In this global environment, the world citizen is entitled to full protection. The General Assembly of the United Nations recognises this, by affirming in a Resolution on the Right to Privacy in the Digital Age\textsuperscript{2327} that the same rights that people have offline must also be protected online. This includes the right to privacy. The resolution also underlines that the protection is endangered due to surveillance practices by states.\textsuperscript{2328}

This resolution pleads for further UN intervention, in addition to the existing general provisions relating to privacy, Article 12 of the Universal Declaration of Human Rights and Article 17 ICCPR. Independently of the UN resolution, further UN intervention also makes sense for substantive reasons. Internally within the European Union, application of the principle of subsidiarity favours intervention at the EU level instead of intervention by the


\textsuperscript{2324} See Halberstam in: Gráinne de Búrca, J.H.H. Weiler (eds), The Worlds of European Constitutionalism (Contemporary European Politics), Cambridge University Press 2012, at 153-163 and the literature mentioned at 157. NB: This ideal is not presented as being based on consensus in the academic world.


\textsuperscript{2327} See also UN General Assembly plenary on 18 December, 2014, Resolution “Right to Privacy in the Digital Age” (A/RES/69/166).

\textsuperscript{2328} The Snowden revelations were the actual trigger for the UN to address privacy in these documents.
Member States, because of the scale and effects of the proposed action.\textsuperscript{2329} On the international scale, the same reasoning would plead for global action, in view of the global nature of the internet.

However, neither the Resolution on the Right to Privacy in the Digital Age nor other recent documents\textsuperscript{2330} of the United Nations call for further action at the level of the UN, but basically refer to the states. Under current law the UN does not impose an obligation on the EU, assuming that the protection given under the Charter complies with the ICCPR. However, a different issue is whether the EU should encourage the UN to play a more prominent role in this area.\textsuperscript{2331} The Special Rapporteur on the right to privacy, appointed by the Human Rights Council of the UN on 3 July 2015, could possibly play a role.\textsuperscript{2332}

\textit{The OECD and its revised Privacy Guidelines: privacy and free flow of information on equal footing}

The OECD is one of the most active organisations in this domain.\textsuperscript{2333} The OECD is an organisation with an economic focus and 34 industrialised countries as members, amongst which a majority of the EU Member States.\textsuperscript{2334} The EU is not a member of the OECD, but is recognised as a partner and is involved – this is a task of the European Commission – in all the activities of the OECD. According to the website of the OECD, the “European Commission’s participation goes well beyond that of an observer”.\textsuperscript{2335}

The involvement of the OECD in privacy and data protection relates to the more general ambition of the OECD to promote policies that will improve the economic and social well-being of people around the world, also taking into account the economic, social and environmental challenges of globalisation.\textsuperscript{2336} Hence, the perspective in the involvement in privacy and data protection is not primarily fundamental rights, as illustrated by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) as amended on 11 July 2013.\textsuperscript{2337}

The guidelines underline the importance of the protection of privacy and, on an equal footing, the free flow of information. They emphasise the need for improved interoperability of privacy frameworks and for cross-border cooperation between privacy enforcement

\textsuperscript{2329} See Chapter 4, Section 3 above.
\textsuperscript{2331} Under the multilateral strategy, see Section 14 below.
\textsuperscript{2332} http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx.
\textsuperscript{2333} Further read, e.g., Lee A. Bygrave, Data Privacy Law, An International Perspective, Oxford University Press 2014, at 43-51.
\textsuperscript{2334} http://www.oecd.org/about/membersandpartners/.
\textsuperscript{2335} To be complete: “While the European Commission’s participation goes well beyond that of an observer, it does not have the right to vote and does not officially take part in the adoption of legal instruments submitted to the Council for adoption”. http://www.oecd.org/about/membersandpartners/.
\textsuperscript{2337} C(2013)79, published on website OECD.
Although the guidelines are not binding, there is a presumption that the members of the OECD, which include, as said, a majority of the EU Member States but not the EU itself, take account of the guidelines within their national jurisdictions. A similar presumption applies to the European Union, derived from EU law. Appropriate cooperation with the OECD, as required by Article 220(1) TFEU, implies that the EU takes these guidelines into account, when acting under Article 16 TFEU.

Moreover, the OECD is a suitable forum for discussion with the United States. The one nuance that can be made in relation to the OECD is that it is composed of industrialised states and hence it is not representative of the less developed countries.

The revised OECD guidelines present a broad consensus between the industrialised states and also include guidance on principles of data protection. Accountability as a modern instrument of ensuring data protection is an important instrument, reinforced by the revision in 2013 and formulated as an obligation for data controllers to put a privacy management programme in place.

The OECD guidelines have been influential, but the fact that they are based on a consensus between essentially different legal frameworks also means that the guidelines are silent on subjects where consensus could not be reached between the EU and its Member States and the US. This is, for instance, the case in relation to the purposes of data processing where the guidelines do not contain requirements on the legitimacy of data processing, as is explicitly mentioned in Article 8(2) Charter.

Apart from the Guidelines, the OECD has also taken initiatives to promote cross-border cooperation in the enforcement of privacy and data protection. In 2007 the OECD adopted a recommendation in that area and in 2010 it facilitated the launch of a Global Privacy Enforcement Network (GPEN), in which a wide range of privacy and data protection authorities cooperate, inside and outside Europe.

6. The Closest Ally, the Council of Europe: The Inspiration for EU Privacy and Data Protection, but Institutionally Difficult

Chapter 2 explained that the ECHR and Convention 108 of the Council of Europe are the inspirations for EU privacy and data protection. The involvement of the Council of Europe in privacy and data protection is purely based on a fundamental rights perspective, which, in

---

2338 Recitals of the Guidelines.
2339 As part of the bilateral strategy. See Section 13 below.
2340 Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013, at 35.
2341 Guideline 15. See on accountability as instrument of EU law, mainly Chapter 6, Section 14 of this study.
2344 See: https://www.privacyenforcement.net.
turn, is closely related to the respect of fundamental rights within the United Nations. As Poullet explains, the Council of Europe is the ultimate guarantor of fundamental rights, imposing on the state a positive obligation to ensure that everyone within the jurisdiction enjoys fundamental rights, also in his relations with private organisations.

Convention 108, adopted by the Council of Europe, has interesting features in relation to privacy and data protection on the internet, since it is more than an agreement between the European states that are members of the Council of Europe. Convention 108 allows accession by non-EU countries. Uruguay used this opportunity. It is a European fundamental rights instrument that can become binding in other continents.

The Council of Europe has 47 European states as its members, including all EU Member States, as well as the Russian Federation and Turkey, which are partly situated in Asia. The European Union and the Council of Europe share a concern for human rights, democracy and the rule of law as fundamental values, but they are separate entities. The relationship between the European Union and the Council of Europe can be characterised as close, yet also complicated.

It is a close relationship. As explained in Chapter 2, the Council of Europe played and still plays an essential role in privacy and data protection in Europe, which largely developed through the case law of the European Court of Human Rights on Article 8 ECHR and with Convention 108 as the first general European instrument for data protection. The case law on Article 8 ECHR and Convention 108 directly influenced the case law of the EU Court of Justice. The European Court of Human Rights is the only non-EU court regularly referred to by the Court of Justice. Moreover, Directive 95/46 on data protection is based on Convention 108. The Convention is an instrument for the control by the DPAs, under Article 8 Charter, if only because beyond the scope of Directive 95/46 – the former first pillar of the EU Treaty – Convention 108 is in many situations the only binding international instrument

---

2347 Article 23 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108. See also Chapter 2, Section 10.
2349 http://www.coe.int/en/web/portal/european-union
2350 Article 23 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.
2351 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981.
the DPAs must take into account. Moreover, ensuring compliance with the national provisions giving effect to the Convention is a task of the DPAs.

It is a complicated relationship, as may be illustrated by the draft agreement on the accession of the European Union to the ECHR, which aimed at finding a balance between two different systems of judicial control. The draft agreement provided for a co-respondent mechanism giving the Union a position before the European Court of Human Rights in cases where a Member State is a party and for a role of the Court of Justice in certain cases to ensure the compatibility with EU law. This complex relationship is also illustrated by the Opinion of the Court on this draft agreement. The EU Court of Justice gave a negative opinion on the Union’s accession to the ECHR provided for in Article 6 TEU. This opinion was characterised as “somewhat formalistic and sometimes uncooperative in defense of its own powers”.

The complicated relationship is also evidenced by two examples in the area of privacy and data protection. The first example relates to the close substantive link between Convention 108 and Directive 95/46. The directive is in many respects a specification of the Convention. However, although ratification by a third country of Convention 108 implies that this third country fulfils the obligations under the Convention, this does not guarantee that the protection provided by the third country is considered as being adequate under Directive 95/46 making it possible that personal data are transferred to this third country without further safeguards. A separate assessment by the European Commission is still needed. The second example is the role of the European Union in relation to the modernisation of Convention 108, initiated by the Council of Europe. It is reported that the Union’s input was aimed at finalising the proposed General Data Protection Regulation of the European Union itself, not at promoting the modernisation of Convention 108.

In short, the ECHR and Convention 108 of the Council of Europe are an inspiration for EU privacy law and may also be instrumental in advancing EU data protection law, also because Convention 108 can become binding upon non-European countries. However, from an institutional perspective the relationship is complicated.

---

2353 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60 does not apply to domestic situations. See Chapter 4, Section 3.
2357 "Editorial comments: The EU’s Accession to the ECHR – a “NO” from the ECJ!", CMLR 2015, pp. 1–15, at 1.
2358 As was in explained in Chapter 2, Section 10.
2360 Christopher Kuner, The European Union and the Search for an International Data Protection Framework, Groningen Journal of International Law, volume 2 number 2, pp. 55-71, 2014, at III.D.
7. A Pluralist Legal Context in the External Domain: The Relation between EU law and International law

This pluralist legal context has three main features, which are relevant for privacy and data protection on the internet. These features are the international competence of the European Union as determined by international law, the internal division of powers within the European Union as determined by EU law, and finally the primacy of international law, albeit subject to limitations. These limitations result from the specific characteristics and the autonomy of EU law, as specified in the Opinion of the Court on the agreement on the Union’s accession to the ECHR, and from the protection of fundamental rights, under the conditions specified in particular in Kadi and Al Barakaat.

These are all features giving substance to the qualification of the Union as an organisation sui generis, also in the international domain.

International competence of the EU: similar but not equal to a state

International law determines the international competence of the Union, as is illustrated by the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations. The European Union has legal personality and is a subject of international law, bound by public international law. It has international competence, recognised under international law.

Externally, the European Union acts similarly to a national jurisdiction, with international legal personality, which has been, since the Lisbon Treaty, formalised in Article 47 TEU. The Union has internal legislation binding upon its citizens and it claims external competences on the internet. It has the competence to conclude agreements with third countries and international organisations, and has concluded numerous agreements. The European Union has – in the same way as a Member State – the capacity to exercise rights under international law, and to enter into obligations.

---

2362 Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461, discussed in various parts of this study.
2363 See, e.g., what is said on the legal personality of the Union, in Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010, at 24-002.
2364 This convention dates from 1986, but did not yet enter into force. However it plays a role in international law. Source: treaties.un.org.
In the area of data protection, the role of the European Union will be even more relevant after the adoption of the General Data Protection Regulation, which will replace national data protection laws. The logical consequence of this should be that in the international domain, too, the European Union is the principal – if not sole – actor, representing the internal acquis in this area.

This role of the European Union – based on EU law – is recognised under international law. The rule is that, due to the very nature of EU law, the European Union in its relations with international organisations has many characteristics of a state. The EU Court of Justice explained that the founding treaties of the European Union have established a new legal order, with its own institutions, limiting the sovereign rights of the Member States and having not only the states but also citizens as its subjects.

However, there are exceptions to the international competence of the European Union. Under international law, the European Union is not always fully assimilated with a state, for instance as far as international responsibility is concerned. It is also not competent to act as a party before the International Court of Justice. In general, “the EU is, under international law, precluded by its very nature from being considered a state”. However, this does not change the fact that in most situations it acts like a state.

Another limitation of the recognition of the European Union in the international domain stems from the fact that the European Union is not a Member of the United Nations. The same applies to the other international organisations that are active in this area, in particular the Council of Europe and the OECD. More generally, full EU membership of the European Union in international organisations is limited. The reticence of the Member States to give up their sovereign position in international organisations is mentioned as the main reason for this. The internal rules of the international organisations determine to what extent the European Union, not being a member, is accepted as an interlocutor.

**Division of powers within the EU: implied powers and exclusive competence**

---

2369 As, e.g., specified by the CJEU in Opinion 2/13, EU:C:2014:2475, at 157. See also 158 and 166.
2370 Although in general the Union “may be held liable if it breaches its obligations and may take action itself where its rights are infringed”, Koen Lenaerts and Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010, at 24-002.
2371 This is a prerequisite for states; Article 34(1) of the Statute of the International Court of Justice.
2374 Just to be complete: the envisaged accession of the EU to the European Convention of Human Rights will not lead to membership of the Council of Europe.
Union law determines the internal division of powers between the Union and the Member State, also where it concerns the exercise of external competence. This means, for instance, that under Article 4(1) TEU the European Union cannot exercise external powers that were not conferred on it by the Member States.

The EU Court of Justice developed the doctrine of implied powers on the basis of AETR. The essence is that the European Union does not only have competences to conclude international agreements that are expressly attributed by the Treaty, but also has implied external powers in areas where internal rules were adopted and even, under certain circumstances, where those rules were not adopted. The latter is the case where an EU competence is needed for attaining a specific objective in the Treaty. The implied external powers of the European Union may be exclusive or shared with the Member States.

This case law was codified in Article 216 TFEU, consolidating the doctrine of implied external powers, developed by the Court. The background of the doctrine of implied powers can either be found in pre-emption (a certain area is occupied by the European Union, hence there is no room for Member States) or in effectiveness of EU law (effet utile).

Simply said, the doctrine of implied powers does not affect the principle of conferral of powers. The doctrine means that where an internal power to legislate exists there also may be an external power to conclude agreements. This is obviously the case for the area of data protection covered by Article 16 TFEU. Article 16 TFEU, read in connection with Article 216 TFEU, implies that the European Union also has external powers in the area of data protection.

Under EU law, it is not fully clear whether the implied powers of the European Union to conclude agreements in the area of data protection qualify as an exclusive or a shared competence. This qualification determines to what extent the Member States are still competent to conclude agreements with third countries on the protection of personal data, or even on other subjects, but with provisions on data protection. One can imagine that Member States might wish to use this remaining competence for the exchange of law enforcement

2376 This is laid down in Article 6 of the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations (1986, but not yet in force, source: treaties.un.org).
2377 Case 22/70, Commission v Council (known as AETR or ERTA), EU:C:1971:32.
2379 Article 216 TFEU is criticised because it potentially limits the case law of the CJEU; The Law of EU External Relations, Cases, Material and Commentary on the EU as an International Legal Actor, P.J. Kuijper, J. Wouters, F. Hoffmeister, G. de Buere and T. Ramopoulos, Oxford University Press 2013, at 19. This criticism is not relevant for this study.
information with third countries, or otherwise for purposes of administrative cooperation with third countries requiring the exchange and use of personal data.

Article 3(2) TFEU addresses the exclusive EU competence for the conclusion of an international agreement.\textsuperscript{2382} The wording of this article is somehow ambiguous, also in relation to Article 216 TFEU.\textsuperscript{2383} Exclusive competence is supposed to exist where an EU instrument explicitly provides for the conclusion of an agreement (this aspect of Article 3(2) TFEU is not ambiguous), but also where the conclusion is necessary for the exercise of an internal competence or where it may affect internal EU law. The term ‘necessary’ requires a stronger justification for exclusive competence than the term ‘may’.

In any event, in our view, the existence of an exclusive EU competence under Article 16 TFEU must be assumed on the basis of the reasoning that effective protection of the fundamental rights of privacy and data protection on the internet cannot be achieved by internal rules alone. Effective protection requires the widest possible geographical scope of protection, and hence external action. The effectiveness or effet utile of the internal regulation justifies exclusive competence for external action. Arguably, the Member States lost their external competence to conclude agreements with third countries on the protection of personal data, or to include provisions on data protection in agreements concerning different subjects. This loss of competence will be even more evident after the entry into force of the General Data Protection Regulation, at least in the areas covered by this instrument.

The exclusive competence could also be based on the theory of pre-emption, in particular after the entry into force of the General Data Protection Regulation, which leaves no autonomy for the Member States to set rules on data protection, except where this is explicitly allowed under the said regulation.\textsuperscript{2384}

At present, the existence of an exclusive competence is less evident. Directive 95/46 leaves more room for the Member States to adopt rules on data protection, it is based on Article 114 TFEU (internal market) and it has as one of its two objectives the free flow of personal data within the internal market.\textsuperscript{2385} This objective does not require an external competence.\textsuperscript{2386} However, this legal basis has lost importance for data protection since the entry into force of the Lisbon Treaty introducing Article 16 TFEU.

\textit{The Charter is silent on territorial application}

\textsuperscript{2382} Article 3(2) TFEU reads: “The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.”

\textsuperscript{2383} The wording is “puzzling” (Piet Eeckhout, EU External Relations Law, Hart Publishing 2011, at 113) and the consequences remain to be seen (The Law of EU External Relations, Cases, Material and Commentary on the EU as an International Legal Actor, P.J. Kuijper, J. Wouters, F. Hoffmeister, G. de Baere and T. Ramopoulos, Oxford University Press 2013, at 19).

\textsuperscript{2384} With the nuances given in Chapter 6, Section 6.

\textsuperscript{2385} Recital (3) of the directive.

The Charter is silent as far as its (extra-)territorial application is concerned.\(^{2387}\) This silence seems to reflect the assumption that the Charter applies to all activities of the Union – and of the Member States when they are implementing EU law\(^{2388}\) – but does not alter the competences of the Union or the Member States.\(^{2389}\) In short, the Charter does not invoke specific concepts of jurisdiction and has no specific field of application.

### 8. Primacy of International Law, Subject to the Specific Characteristics and the Autonomy of EU Law

Where the European Union uses its competence to conclude an agreement on privacy and data protection, under Article 16 TFEU, read in connection with Article 216 TFEU, it acts under international law. In addition, the Union should consider the case law of the Court of Justice on the limits of external competence and of the primacy of international law.

In its Opinion on the agreement on the accession of the European Union to the ECHR,\(^{2390}\) the Court ruled that the accession to the ECHR as provided for in that agreement was not compatible with EU law, because it did not take sufficient account of the specific characteristics and the autonomy of EU law.

An essential element in the reasoning of the Court relates to what the Court called the “very concept of external control”\(^{2391}\) by a court that is not part of the EU legal system. Although external control would in principle be allowed it should not result in a situation where the findings of the Court in relation to the application of the Charter by the Member States could be put into question,\(^{2392}\) nor where “the level of protection provided for by the Charter or the primacy, unity and effectiveness of EU law”\(^{2393}\) is compromised.

It is the Court itself that ultimately – and in last resort exclusively – interprets the Charter and more generally EU law. This is relevant for the subject of this study, because this position of the Court may impose limits on the powers of the Union to conclude an international agreement on standards for privacy and data protection if such agreement were to provide for some kind of international dispute settlement regime that would be binding upon the European Union and its Member States. Dispute settlement mechanisms are common in trade agreements, for instance in the context of the World Trade Organization.\(^{2394}\)

\(^{2387}\) In this respect, it differs from the ECHR, which in Articles 1 and 56 deals with the territoriality of protection.

\(^{2388}\) As interpreted by the CJEU, e.g., in Case C-617/10, Åkerberg Fransson, , EU:C:2013:280.


\(^{2390}\) CJEU, Opinion 2/13, EU:C:2014:2475.

\(^{2391}\) At 185 of the opinion.

\(^{2392}\) At 186 of the opinion, more precisely formulated.

\(^{2393}\) At 188 of the opinion, quoting Case C-399/11, Melloni, C:2013:107, at 60.

Legal effect of international law within the EU legal order and the respect of EU fundamental rights in the Kadi case law

Article 216(2) TFEU provides that agreements concluded by the European Union are binding on the institutions as well as on the Member States. Article 216(2) TFEU is silent on the possible direct effect of provisions of international agreements, binding individuals and legal persons. Eeckhout explains this extensively.\textsuperscript{2395} Direct effect is, in the first place, used to denote the effect on the legal order of the Union. If a provision of an agreement has direct effect, it should be applied by the European Union and possible inconsistent internal EU law is overridden. Furthermore, since the provision is integrated into the EU legal order, it subsequently applies directly in the national atmosphere, if necessary, overriding inconsistent national law. De Búrca describes this approach as automatic incorporation, based on an attitude of notable openness and with the Court of Justice in a role as faithful enforcer of international obligations within the EU legal order.\textsuperscript{2396}

The Court of Justice nuanced in Kadi and Al Barakaat\textsuperscript{2397} the direct effect of provisions of international agreements. According to the Court, obligations under international law cannot have the effect of prejudicing the constitutional principles of the Treaties.\textsuperscript{2398} The Court gave a further specification in Commission and others v Kadi (Kadi II), \textsuperscript{2399} in which it ruled that on the one hand “the primacy of a Security Council resolution at the international level” should not be “called into question”, but that, on the other hand, this must not “result in there being no review of the lawfulness of such European Union measures [based on a Security Council resolution]\textsuperscript{2400} in the light of the fundamental rights which are an integral part of the general principles of European Union law.”

There is abundant literature on the Kadi jurisprudence\textsuperscript{2401} and on its role in determining the relationship between the international legal order and the EU legal order. For a basic understanding, it is instructive to highlight the difference of approach between the General Court and the Court of Justice.\textsuperscript{2402} In the view of the General Court, a unity exists between international and EU law, and within this unity there is a strict hierarchy between international law and EU law. This does not mean that the EU Courts must obediently apply...
international agreements, but their scrutiny is limited to the question as to whether such an agreement infringes a higher principle of international law, known as *jus cogens*.\textsuperscript{2403}

This reasoning was overruled in appeal by the Court of Justice. The Court construed obligations under international law within the internal EU framework that require the respect of some basic values, such as the respect of fundamental rights recognised under EU law. In *Commission and others v Kadi (Kadi II)*\textsuperscript{2404} the Court specified that it is its task, as far as international agreements are concerned, to ensure the review, in principle the full review, of the lawfulness of all Union acts in the light of the EU fundamental rights.

In the approach of the highest EU Court, the higher principles of law that may override an internationally agreed provision stem from the internal EU legal order, not from international law. It is important to keep this in mind, where internet privacy and data protection are at stake. According to this case law, EU concepts on fundamental rights prevail, whenever this is necessary, over international law. EU law contains principles that must be respected in the international domain, are not negotiable and subject to full review of the EU Courts.

This approach of the Court of Justice has a certain similarity with the case law of the German constitutional court relating to the primacy of EU law.\textsuperscript{2405} This similarity is caused by the fact that the primacy of the ‘higher’ law is accepted, but that it is the court of the ‘lower’ jurisdiction that ultimately decides whether this is the case (or not). At the end of the day the Court of Justice has the power to invalidate the application within the EU legal order of provisions in international agreements, albeit only for reasons of fundamental rights protection.\textsuperscript{2406}

9. Jurisdictional Issues: Public International Law and the Internet

Jurisdiction is founded in public international law as well as in private international law. This study focuses on public international law, in line with the perspective of the study, the role of the European Union as a guardian of privacy and data protection. This focus of scope is made whilst fully recognising that private international law is relevant for data protection, in particular because private international law determines the applicable law or the competent court, in cases where a company or an individual engages in a law suit under private law. This study also recognises commentators noting that data privacy blurs the distinction between public law and private law.\textsuperscript{2407}

\textsuperscript{2403} This is an indirect judicial review, which may “highly exceptionally, extend to determining whether the superior rules of international law falling within the ambit of jus cogens have been observed”, Case T-315/01, *Kadi v Council and Commission*, EU:T:2005:332, at 231.

\textsuperscript{2404} Joined cases C-584/10 P, C-593/10 P and C-595/10 P, *Commission and others v Kadi (Kadi II)*, EU:C:2013:518, at 97.

\textsuperscript{2405} As explained in Chapter 4, Section 13 of this study.

\textsuperscript{2406} In the case law of the German constitutional court the ‘*ultra vires*’ action of the EU is also predominant, but that aspect is not relevant here.

\textsuperscript{2407} Further read: Extraterritorial Data Privacy Law, Dan Jerker B. Svanessøn, 2013, at 2.2.
A third foundation of jurisdiction is the jurisdiction laid down in international fundamental rights treaties, imposing extraterritorial obligations on states to protect individuals, even where there would be no jurisdiction in public international law and the state has no power to act. This foundation of jurisdiction in international human rights law may be relevant for the exercise of jurisdiction based on Article 8 ECHR, on Convention 108 or on Article 17 ICCPR. However, as Moreno-Lax & Costello explain, this foundation of jurisdiction is controversial and – as they underline – ill-fitting in the EU context. This argument is not necessarily undisputed, but, this study – which does not address jurisdiction as a core topic – does not further elaborate on international human rights law jurisdiction.

EU jurisdiction under public international law: a wide power to prescribe

Under public international law, there is no generally accepted solution for internet jurisdiction. One must rely on general public international law. In public international law, jurisdiction means a limitation of states to act, because of sovereign claims of other states. The main rule of jurisdiction is that the jurisdictional competence of a state – or the European Union, which in this particular context equals a state – is primarily territorial. Within its territory, the state has exclusive power to enact and to enforce the law.

The power of a state outside its territory was defined in 1927 by the Permanent Court of International Justice, in Lotus. This case is still the main standard of reference for jurisdiction. Lotus made a distinction between enforcement and prescriptive jurisdiction. The rule is that “States are precluded from enforcing their laws in another State’s territory”, but “international law would pose no limits on a State’s jurisdiction to prescribe its rules for persons and events outside its borders”.

In an era of globalisation, the exercise of extraterritorial jurisdiction is often inevitable. On the internet, the European Union is vulnerable due to adverse effects of foreign activities in the internal EU legal order. This vulnerability justifies extraterritorial jurisdiction in an internet environment. Article 4(1)(c) of Directive 95/46 is an example of how the European Union establishes extraterritorial jurisdiction to address these adverse effects by

---


2410 Milanovic, referred to by Moreno-Lax and Costello attaches more importance to fundamental rights jurisdiction.


2413 Cedric Ryngaert, Jurisdiction in International Law, United States and European Perspectives, Doctorate Thesis Katholieke Universiteit Leuven, 2007, at 35.

2414 Cedric Ryngaert, Jurisdiction in International Law, United States and European Perspectives, Doctorate Thesis Katholieke Universiteit Leuven, 2007, at 770.

2415 The directive applies where “the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State […]”. 418
bringing data controllers in third countries, who make use of equipment in the European Union, within the scope of EU law.

Other bases for jurisdiction outside the territory of a state have been recognised, all founded on the notion that there must be a meaningful link with the state claiming competence. Some other bases are: nationality, flag, diplomatic and consular relations, effect, protection, passive personality and universality. These bases do not all have the same relevance for the subject of this study. Obviously, diplomatic and consular relations are not directly relevant for privacy and data protection on the internet. The same could probably be said about passive personality, used in criminal law as a basis for a state to protect its citizens abroad. The passive personality principle allows states, in limited cases such as terrorism, “to claim jurisdiction to try a foreign national for offenses committed abroad that affect its own citizens”. Also a flag is not directly relevant on the internet in view of its networked nature. The following bases for the European Union to claim jurisdiction outside of the EU territory could, however, be relevant: nationality, effect, protection and universality, as will be discussed below.

The exercise of jurisdiction on these bases is limited by sovereign territorial rights of other states. An example is the exercise of jurisdiction on the basis of personality over nationals abroad. This exercise is subordinate to the territorial competence of the other state concerned and, in principle, the latter’s consent is required.

In addition, for the European Union, the exercise of extraterritorial competence is – just like any action of the European Union – subject to the principle of effectiveness. In principle, this exercise of jurisdiction is only legitimate if there is effective control over the persons or activities outside the territory, a requirement that acquires a new dimension on the internet. Laws on the internet must actually be enforceable, otherwise this would undermine the trust in the legal system. However, this does not per se exclude a wider claim of jurisdiction.

---

2416 This list is taken from the ruling of the ECtHR in Bankovic v Belgium, Application No. 52207/99, at 59. See also: Violeta Moreno-Lax and Cathryn Costello in: The EU Charter of Fundamental Rights, A Commentary, Edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward, Hart Publishing 2014, at 1667. B. Mayer (note on Case C-366/10 - Air Transport Association of America and Others, EU:C:2011:864, CMLR 49 (2012), 1113–1140) criticised the CJEU for another reason: not following the line of Kadi and taking into account environmental protection as a fundamental right (which would have led to similar outcome in the case, but for different reasons).

2417 Further read: Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing 2013.


2419 This perspective of applicability of EU law means that this section is not about internet jurisdiction on general, which would cover also other methods to establish jurisdiction, such as the choice of law. See on this: Joel R. Reidenberg, “Technology and Internet Jurisdiction”, University of Pennsylvania Law Review, vol. 153/1951 (2005).

2420 ECtHR in Bankovic v Belgium, Application No. 52207/99, at 60.


2422 Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing 2013, at 70.
where the European Union has no power to enforce. Svantesson makes a difference between “bark-jurisdiction” and “bite-jurisdiction”.2423

Especially in a rapidly developing information society, the European Union – acting as a state – could also claim extraterritorial jurisdiction in accordance with public international law, in situations where – at this stage of development – effective enforcement is not guaranteed or even absent. This claim makes sense, for two reasons. First, the European Union underlines the values it defends in an internet environment, which could encourage interlocutors in third countries to comply ‘voluntarily’. Second, the absence of effective enforcement power does not mean that enforcement power will not evolve in the immediate future.

*The respect of territorial sovereign rights: overlapping jurisdictions in cyberspace but a wide discretion for the EU legislator*

The territoriality principle is the most basic principle of international jurisdiction, meaning that a state has jurisdiction over acts that have been committed within the territory.2424 Territoriality, however, does not fully work on the internet as a global network, or – with reference to Castells2425 – a networked society.2426 The overlapping of jurisdictions on the internet is no longer an exception, but it is the essence of the internet as a global network itself. This is the background for a short exploration of alternative grounds of jurisdiction.

In a paper on extraterritorial jurisdiction in cyberspace,2427 Hildebrandt discusses alternative grounds of jurisdiction. The first alternative she refers to is to compare the internet to the freedom of the seas, as developed by Grotius in his *Mare Liberum*, first published in 1609. In line with the view of Grotius, the internet should be a free space – or a common good – where national laws do not apply. This view was found attractive by scholars in the earlier age of the internet, like Johnson & Post who rightly claimed in 1996 that the internet “radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules”.2428 Consequently, the internet should be governed by a separate body of law. This claim provoked a debate between Goldsmith and Post on this point, in which Goldsmith claimed that the internet is functionally identical to other transnational activities, the traditional legal tools being applicable, and Post replied that this was not the case.2429

---

2424 Cedric Ryngaert, Jurisdiction in International Law, United States and European Perspectives, Doctorate Thesis Katholieke Universiteit Leuven, 2007, at 47.
2425 Manuel Castells, The Rise of the Network Society, Volume I: The Information Age: Economy, Society and Culture, 2nd edition (2010), as explained in Chapter 3, section 4 of this study.
2426 Further read: Mireille Hildebrandt, Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace, University of Toronto Law Journal, Volume 63, Number 2, Spring 2013, pp. 196-224.
2427 Mireille Hildebrandt, Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace, University of Toronto Law Journal, Volume 63, Number 2, Spring 2013, pp. 196-224.
In our view, the argument that the internet should be governed by a separate body of law certainly has its merits, but is at present difficult to reconcile with the pervasiveness of the internet in our daily lives. It makes ever less sense to consider the internet as a space that can be separated from the physical world. RFID, the Internet of Things and the ubiquitous connectivity through mobile devices are logical illustrations. Another example, which is illustrative for jurisdiction, is that the internet facilitates cross-border remote control.

Another alternative ground for jurisdiction in Hildebrandt’s paper is what she calls “occupatio”. Where interests of sovereign states are a stake, states take the law into their own hands and enforce the law outside their physical borders. The hacking of a computer system located abroad for law enforcement purposes is an example. Another example is provided by the practices revealed by Snowden, which demonstrate that surveillance by the NSA also takes place outside US territory.

The case law on internet jurisdiction is still limited. This is why the case law in areas with similarities to the internet has relevance. Air Transport Association of America and Others concerned the sovereignty over the airspace. In this case, the European Court of Justice ruled on EU legislation giving wide territorial effect to the EU measures on greenhouse gas emissions trading schemes, based on the Kyoto Protocol, by applying these measures to all flights departing or arriving in the European Union. The Court accepted this wide territorial effect, which led to criticism, in view of the extensive interpretation of public international law by the Court.

This leads to a further starting point for the examination of internet jurisdiction. The EU legislator has a wide margin of discretion in laying down provisions with extraterritorial effect. However, these provisions cannot by themselves enlarge the powers of the European Union under public international law. Legitimate claims by third countries and international organisations should be respected. A prima facie – in line with Air Transport Association of America and Others – the Court of Justice interprets this limitation strictly. It is in this context that the active role entrusted to the European Union for the protection of the fundamental rights of privacy and data protection must be reconciled with public international law.

---

2431 Mireille Hildebrandt, Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace, University of Toronto Law Journal, Volume 63, Number 2, Spring 2013, pp. 196-224, at 204.
2432 Illustrations of extraterritorial State practices on Internet are found in Eric Schmidt, Jared Cohen, The New Digital Age, 2014.
2433 Case C-366/10, Air Transport Association of America and Others, EU:C:2011:864.
2435 Case C-366/10, Air Transport Association of America and Others, EU:C:2011:864.
10. **Jurisdiction Should be Based on a Meaningful Link with the Protection of Individuals in the EU: The Effect of an Act on the Internet on Individuals residing in a Jurisdiction**

The case law on internet jurisdiction is still limited and there are no clear international rules under public international law. The international instruments on private international law, such as the United Nations Convention on the Use of Electronic Communications in International Contracts, do not give a clear indication on internet jurisdiction either.\(^{2436}\)

This means that a solution is required for a problem that the Court of Justice already recognised in *Lindqvist*.\(^{2437}\) In principle, every publication on a website by a public or private actor based in a third country containing personal data that can be accessed within the European Union has an effect in the Union and could thus trigger the applicability of EU data protection law.

In theory, the European Union could, therefore, claim jurisdiction over the entire internet. Kuner mentions the example of the publication by a company in China of the payroll data of its employees, who are all residing in China.\(^{2438}\) This publication is accessible from the Union, but the link with the Union is very weak and claiming jurisdiction would be difficult to justify, whereas there is a legitimate claim of jurisdiction by a third country that should be respected.

This example shows that any – theoretical – effect would not be enough to claim EU jurisdiction, but that a stronger effect on the privacy and data protection of individuals within the European Union is needed to establish jurisdiction for EU law. Above, we explained that public international law, as interpreted in *Lotus*,\(^{2439}\) does not limit the prescriptive jurisdiction of a state (nor of the Union) and allows the simultaneous exercise of a multiplicity of jurisdictions. An alternative presented by Ryngaert is the conferral of jurisdiction on the state with a strong link, or even the strongest link, with the matter to be regulated. In privacy and data protection, this strong link could be based on the need for effective protection of individuals in the Union. Reformulated, a legitimate claim of external EU jurisdiction in this area should be based on a meaningful link with the effective protection of the individual in the European Union.

A meaningful link with the protection in the European Union could be established by alternatives for territorial jurisdiction, such as jurisdiction based on nationality, effect,

---


\(^{2437}\) Case C-101/01, *Lindqvist*, EU:C:2003:596, at 56-71. In Lindqvist the CJEU ruled on a situation of uploading of personal data on the internet, by a European resident. The CJEU dealt with the question arose this simple uploading automatically means a transfer of personal data to third countries.


protection and universality.\textsuperscript{2440} In the literature on internet jurisdiction the emphasis is on personal jurisdiction, based on the need to protect individuals in view of the effect an act on the internet has on individuals residing in a jurisdiction. Reidenberg a.o. analyse personal jurisdiction, based on a test of effects. This test has similarities with a test based on the need for protection of the persons falling within the jurisdiction.\textsuperscript{2441} The test combines components of nationality, effect and protection. Universality is not claimed, because universality would amount to establishing jurisdiction over the entire internet.

The first relevant element of the test is nationality or personal jurisdiction based on residence. The relationship in data protection law between nationality, citizenship, residence or any other link of a person to the jurisdiction of the European Union has not been clarified in EU law. The TFEU and the Charter confer the right to data protection on “everyone”. This means that nationality – or EU citizenship based on the nationality of a Member State\textsuperscript{2442} – is not the condition for protection under EU law.\textsuperscript{2443} Everyone is entitled to protection, but there is a limitation, because it is only within the scope of EU law that individuals are entitled to protection. However, this limitation does not precisely circumscribe jurisdiction, in view of the borderless nature of the internet.

The second relevant element of the test is based on the doctrine of effect for claiming territorial jurisdiction. This doctrine was the basis for a ruling of a French court ordering Yahoo! to prevent the access in France of webpages with Nazi material, coming from the United States.\textsuperscript{2444} The ruling was criticised as a threat to the freedom of expression because it resulted, on the basis of the doctrine of effect, in the restriction of the dissemination of content it regulated.\textsuperscript{2445} However, this ruling did have a positive effect from the perspective of protection, as has been argued by Reidenberg.\textsuperscript{2446} The ruling empowers a state – in casu France – to protect its values on the internet, because of the effect of the publication in this state.

The doctrine of effect is closely linked to personal jurisdiction based on residence. There is case law recognising that a statement on the internet affecting persons in other countries is sufficient to establish jurisdiction. A case often mentioned in literature is the ruling of the High Court of Australia in Dow Jones v Gutnick\textsuperscript{2447} on a defamation in a US web magazine

\begin{itemize}
  \item \textsuperscript{2440} See Section 9 above.
  \item \textsuperscript{2441} Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law (Fordham Center on Law and Information Policy, 2013). This survey gives an overview of case law, with a focus on the US. The angle is mainly private international law.
  \item \textsuperscript{2442} As laid down in Article 20 TFEU. See also Chapter 4, Section 9 of this study.
  \item \textsuperscript{2443} Kuner in: Data protection anno 2014: how to restore trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), Hielke Hijmans and Herke Kranenborg (eds), Intersentia 2014, at 219.
  \item \textsuperscript{2444} Joel R. Reidenberg, The Yahoo! Case and the International Democratization of the Internet, Fordham Law & Economics Research Paper No. 11, 2001.
  \item \textsuperscript{2445} Brendan Van Alsenoy and Marieke Koekkoek, Internet and jurisdiction after Google Spain: the extraterritorial reach of the ‘right to be delisted’, International Data Privacy Law, 2015, Vol. 5, No. 2, at 110..
  \item \textsuperscript{2447} Dow Jones v Gutnick (2002) 210 CLR 575 (Australia), as described by Dan Jerker B. Svantesson, Extraterritorial Data Privacy Law, 2013, at 34-39, and by Joel R. Reidenberg, “Technology and Internet
\end{itemize}
posted in the US, affecting an individual in Australia. The High Court mentioned the uniquely broad reach of the internet, and accepted jurisdiction in Australia. It was criticised for that, because it extends the liability for speech to a wide range of foreign laws.\footnote{Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law (Fordham Center on Law and Information Policy, 2013), at 25-26.}

A solution for limiting this wide effect is the use of geolocation technologies, specifying the access to content according to the location of the internet user.\footnote{Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law (Fordham Center on Law and Information Policy, 2013), at 16-17.} It is a solution enabling countries to assert jurisdiction over acts conducted abroad and at the same time to limit the impact of its jurisdiction to its own territory.\footnote{Brendan Van Alsenoy and Marijke Koekkoek, Internet and jurisdiction after Google Spain: the extraterritorial reach of the ‘right to be delisted’, International Data Privacy Law, 2015, Vol. 5, No. 2, at 114.} This solution also plays a role in the follow up of Google Spain and Google Inc.,\footnote{Case C-131/12, Google Spain and Google Inc., EU:C:2014:317} in relation to the technical possibility to prevent internet users in Europe from accessing search results on Google.com that have been delisted in the European versions of Google.\footnote{The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015, \url{https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNhDA/view}, at 5.4.} This possibility has been criticised: geolocation technologies are said to threaten the open nature of the internet,\footnote{Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law (Fordham Center on Law and Information Policy, 2013), at 16-17.} leading to fragmentation of the internet,\footnote{Joel R. Reidenberg a.o., Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law (Fordham Center on Law and Information Policy, 2013), at 16-17.} and would allow repressive regimes to censor search results.\footnote{See Chapter 3, Section 4.}

This criticism relates to the global and borderless structure of the internet and more particularly to the fact that any governmental action has an external effect, and hence has an impact on the discretion of other jurisdictions to regulate the internet according to their (constitutional) preferences. An even further reaching argument is that intervention by the Union (or national governments) based on European or national values would not be in conformity with the internet as a global, unfragmented environment. The criticism is rebutted by the argument of Reidenberg mentioned above: a state must be empowered to protect its constitutional values on the internet. If not, the state is not able to exercise a core task: the effective protection of the fundamental rights of citizens. Just to recall, the perceived lack of protection on the internet as a result of big data and mass surveillance is one of the triggers of this study.\footnote{See Chapter 1 of this study.}

The Commission Proposal for a General Data Protection Regulation\footnote{Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.} addresses this need for effective protection, although it is not very precise. Recital 12 states: “The protection
afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.” However where the controller is based outside the European Union, it only applies to EU residents when goods and services are offered to them or their behaviour is being monitored. The contribution of the Council contains an interesting specification: the monitoring of their behaviour is only covered as far as their behaviour takes place within the European Union. An EU citizen travelling in the United States would, in the perception of the Council, thus not protected against monitoring. However, there is no communis opinio as to whether the EU citizen travelling in a third country is protected by EU law when goods and services are offered to him or her.

On the basis of these considerations, we conclude that a meaningful link with the European Union could consist of personal jurisdiction based on residence and the doctrine of effect, legitimising extraterritorial effect. This study suggests that, in the external domain, the Union should promote this foundation of (personal) jurisdiction in international organisations, aiming at ensuring that individuals are effectively protected within their jurisdiction, but without the result that the entire internet falls within the scope of a specific jurisdiction, such as EU law. This suggestion does not aim at solving the problem of internet jurisdiction, but could be included in the EU action on the international scene in the area of privacy and data protection.

11. Articles 3(5) and 21 TEU as the Starting Point for EU Action on the International Scene in Privacy and Data Protection

Introductory remarks

Articles 3(5) and 21 TEU specify that the European Union has an active role in upholding and promoting democracy, the rule of law and fundamental rights. In the Laeken Declaration of 2001, the European Council positioned the Union as a “power seeking to set globalisation within a moral framework”, emphasising the need of taking responsibility for globalisation. Cremona calls this the role of the Union as stabiliser of the world. Bradford states that this role is based on the claim that these values of the Union are “normatively desirable and universally applicable”.

This active role of the European Union in upholding and promoting its core values is the starting point for the approach of the Union in privacy and data protection. In this approach,

---

2458 Article 3(2) of the Commission Proposal for a General Data Protection Regulation. Also Article 41(2) and (5) mentions this specific category.
2459 This addition from the Council is also included in Consolidated text (outcome of the trilogue of 15/12/2015), available on http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884.#
2460 European Council, Presidency conclusions - Laeken, 14 and 15 December 2001, incl. Annex I Laeken Declaration on the future of the European Union, at 20, also pointing at glorious European events, the Magna Carta, the Bill of Rights, the French Revolution and the fall of the Berlin Wall.
the ambition to promote and apply EU data protection law extraterritorially plays an important role.\footnote{Kuner even speaks about an apparent decision to do this, Christopher Kuner, The European Union and the Search for an International Data Protection Framework, Groningen Journal of International Law, volume 2 number 2, pp. 55-71, 2014, at IV.1.}

Article 21 TEU does not only specify principles for EU action, in particular democracy, the rule of law and human rights, it also lays down that the Union should seek partnerships with democratic third countries and organisations. These partnerships are a vehicle for enhancing a global level of democracy, the rule of law and the protection of human rights.

In the area of privacy and data protection, the logical options for such a partnership would be a close cooperation between the EU and the US, as jurisdictions sharing the main aspirational goals,\footnote{David C. Vladeck, A U.S. Perspective on Narrowing the U.S.-EU Privacy Divide, in “Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime, Artemi Rallo Lombarte, Rosario García Mahamut (eds), Tirant lo Blanch, 2015.} and closer cooperation within the OECD. The common aspirational goals are elaborated in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.\footnote{1980, as amended on 11 July 2013 by C(2013)79.} Moreover, both jurisdictions, as well as the OECD, face similar challenges as a result of the main developments in the information society. Big data, as well as the surveillance practices revealed by Snowden, are the logical examples of such challenges.\footnote{Further read: “Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions”, Amsterdam / Cambridge, September 2015, https://www.cbpweb.nl/sites/default/files/atoms/files/privacy_bridges_paper.pdf.}

Of course, the most obvious candidate for a partnership in the area of privacy and data protection would be the Council of Europe. The Council of Europe did not only set the standard for privacy and data protection in the European Union and within the whole European continent, it also opened Convention 108\footnote{Article 23 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.} for accession by non-European countries. As mentioned above, Uruguay was the first non-European country to accede in 2013.

The following sections of this chapter specify the impact of the ambitions of the European Union in the external arena. The fact that the Union is an organisation based on the values of democracy, the rule of law and fundamental rights, determines the content of the action as well as the choice of the most promising strategy.

Roughly speaking, the European Union can choose between three strategies for the protection of fundamental rights in the international domain. The strategy can be primarily unilateral, aimed at exporting EU norms to the rest of the world, bilateral by seeking arrangements with like-minded countries or multilateral, through arrangements on a global scale.

\textit{Strategies for the EU in the international domain}
In simple terms, individuals cannot be effectively protected, if the protection ends where their personal data are processed outside the EU territory or where they interact on the internet with parties outside this territory. Hence, this calls for the European Union to act in the international domain.

In a paper called “The Brussels Effect”, Bradford argues that the European Union has global power through its legal standards and also through its legal institutions. The Union is successful in exporting these standards and hence influencing the rest of the world. This exercise of regulatory power by the Union compensates for a – compared to the US – relatively weak military power. One of the examples Bradford explores in support of this argument is the area of privacy and data protection. Her paper serves as an inspiration for the next sections of the study, which discuss the possibilities of successful EU strategies in the international domain.

The three strategies are: a unilateral, a bilateral and a multilateral strategy, whilst not excluding that, in practice, a smart mix of these three strategies would be the best option. The Safe Harbour decision of the European Commission, which was based on the adequacy of the protection in the US as determined under EU law (unilateral) but also includes a commitment of the government of the United States (bilateral), can be seen as illustration of a mix of strategies.

This study expresses a preference for the unilateral strategy, at least at the short term, realising that this strategy has its weaknesses. As Ryngaert explains, a unilateral strategy is also linked to skepticism as to whether third countries and international organisations are able to deliver protection in an acceptable manner. “Often, extraterritoriality is informed by a vague sense of superiority or exceptionality of domestic law”, so he states.

12. **Unilateral Strategy: A Potentially Successful Approach**

The unilateral strategy aims at exporting EU values and arrangements in a unilateral way, not by negotiating with third countries or international organisations. The rationale of this strategy is the idea that protection will be best guaranteed by the unilateral application (“export”) of the system that guarantees the highest level of protection. If certain market conditions are fulfilled, global actors will adapt to this level. This phenomenon is described in

---

2469 To be complete, she also mentions legal institutions of the EU in this context.
2471 Cedric Ryngaert, Jurisdiction in International Law, United States and European Perspectives, Doctorate Thesis Katholieke Universiteit Leuven, 2007, at 771.
It is the opposite of the “race to the bottom” or the “Delaware effect”, where the lowest common denominator determines the level of global standards.

In the area of privacy and data protection the highest level is mainly, but not necessarily in all aspects, guaranteed by the European Union. Moreover, there is evidence that most countries adopting data protection laws, also outside Europe, are following the main standards of the European Union (and of the Council of Europe) and that the United States with its different system is becoming increasingly isolated. Bradford formulates five conditions for the success of this unilateral strategy.

The first condition is a relatively powerful internal economy. This condition seems to be fulfilled, in view of the size of the European market and the tendency for globally operating companies to comply with the rules of the regions that have the most stringent approach (“race to the top”), provided that these regions have market power. The relatively important consumer market of the European Union represents the powerful internal economy. This relative importance may be adversely affected by the emerging economies elsewhere in the world, with China as an emerging economy that is reported as not following the main EU standards on data protection. However, the EU consumer market remains important.

The second condition is a strong regulatory capacity. This condition does not only include enactment, but also enforcement power. In itself there is no reason to doubt the regulatory capacity of the European Union. On the contrary, Bradford’s paper is based on the presumption that the Union possesses a strong regulatory capacity. The perceived weakness of (some) DPAs in the Union may, to a certain extent, be an impediment to the fulfilment of this condition, at least until the entry into force of the General Data Protection Regulation, which will further empower these authorities and strengthen their cooperation.

The third condition is a political will to deploy strict rules. The negotiations on the General Data Protection Regulation demonstrate the political willingness to reach a result in order to ensure strong data protection. The European Parliament, the Council and the European Commission...
Commission are all committed to the outcome, although the difficult negotiations reveal that within the EU institutions and, in particular in the Council, differences exist as to the desirable level of protection.

The fourth condition is a relatively inelastic market where the object of regulation cannot simply relocate. If one defines the relevant market as the consumer market, this condition is fulfilled. The market is inelastic because consumers will not move outside of the European Union to escape strong data protection standards.

The fifth and final condition is the non-divisibility of standards, which makes it unattractive for companies to distinguish their policies depending on the region of the world. This condition is directly related to the issue of fragmentation of the internet. As long as the main operators on the internet do not distinguish the essence of their operations between the different regions of the world, this condition is fulfilled. However, a unilateral strategy by the European Union could also lead to fragmentation. This would not necessarily prejudice the level of privacy and data protection in the Union, but may have undesired side effects, for instance for internet freedom.

In short, on the basis of the conditions of Bradford the unilateral strategy is a potentially successful approach. The European Union has regulatory clout and manages to unilaterally set the global standards for regulation on privacy and data protection in many areas. The Union is to a certain extent capable to ‘export’ its system on privacy and data protection and has assumed leadership in the global regulation of data privacy. The Union could – as part of the unilateral strategy – use facilities offered by the Council of Europe, such as the possibility that non-European countries adhere to Convention 108.

Most OECD countries follow the EU system of data protection, which is characterised by a generic legislative framework and independent authorities. The US system is more of an exception amongst these countries. To the extent the Union’s regulatory clout is dependent on

---

2480 See, e.g., Chapter 6, section 3 of this study.
2481 In a general fashion, not entering the specificities of market definition under EU competition law, which usually defines markets related to specific products or services.
2482 Internet Balkanization gathers pace: is privacy the real driver?, Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, and Orla Lynskey, International Data Privacy Law, 2015, Vol. 5, No. 1. See Chapter 3, Section 4.
2483 Bradford argues that this is indeed the case, for technological as well as for cost related reasons; Anu Bradford, “The Brussels Effect”, 2012 Northwestern University Law Review Vol. 107, No. 1, at 25.
2484 Obviously there is a close link to the debate following Case C-131/12, Google Spain and Google Inc., EU:C:2014:317, evoked in various parts of this study.
2485 Most OECD countries follow the EU system of data protection, with a generic legislative framework and independent authorities. The US is more of an exception.
2486 This is well described by Bach & Newman, Yale Law School Legal Scholarship Repository, Faculty Scholarship Series - Yale Law School Faculty Scholarship, 1-1-2004, http://www18.georgetown.edu/data/people/ala24/publication-22020.pdf.
2487 As explained in Section 6, also mentioning that Uruguay did adhere.
the relative importance of the European market, the rise of emerging markets may limit this position in the future.

The analysis of Greenleaf on the influence of European data privacy standards outside Europe gives a further illustration of the potential of a unilateral strategy, in a list of indicators of European influences on non-European data privacy laws.\textsuperscript{2488} Following this strategy does not exclude that, on a practical level, bridges may be built with like-minded countries, finding communalities for joint challenges relating to internet privacy.\textsuperscript{2489} It also does not exclude the adoption of global technological solutions based on international technological standards that encourage protection on a global level, and that respect differences in legislation.\textsuperscript{2490}

13. Bilateral Strategy: Joining Forces with Like-minded Jurisdictions such as the US

The bilateral strategy roughly involves seeking for arrangements with relevant, like-minded jurisdictions, such as the US, and, by doing so, building bridges between these jurisdictions. This strategy has attractive features. In the first place, the strategy avoids what may be perceived from the US side as regulatory imperialism by the EU.\textsuperscript{2491} In the second place, the strategy may have benefits to the benefit of global privacy and data protection. A cooperation between the EU and the US jurisdictions – whether or not by way of formal treaties – would be a means to face common challenges in the area of privacy and data protection in a coordinated manner and to allow both parties to join forces, for instance in the field of enforcement. In the third place, if well negotiated, the strategy might encourage the US to adopt the standards originating from the EU and hence be instrumental to the fulfilment of the EU’s task under Articles 3(5) and 21 TEU to uphold and promote its values in the wider world. In the fourth place, the strategy might create a level playing field between companies operating from the US and those operating from the EU and, by doing so, contribute to ensuring the competitive position of EU companies.\textsuperscript{2492} In the fifth place, if the great powers act in concert, this is a more effective way of policy-making and harmonisation in a global environment than is the case where these powers fail to agree.\textsuperscript{2493}

\textsuperscript{2489} This is the subject of the “Privacy Bridges”-project. See: “Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions”, Amsterdam / Cambridge, September 2015, https://www.cbpweb.nl/sites/default/files/atoms/files/privacy_bridges_paper.pdf.
\textsuperscript{2490} This is one scenario, in De Hert, P. and Papakonstantinou, V., “Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?”, A Journal of Law and Policy for the Information Society, vol. 9, no. 2, 2013, 271-324, at 308-310. ISO standards are mentioned at 295-296.
\textsuperscript{2492} According to Cremona, this is an important driver behind EU policies, Marise Cremona, “The Union as a global actor: Roles, models and identity” CMLR 41, pp. 553–573, at 556.
\textsuperscript{2493} In this sense, Daniel W. Drezner, Globalization, Coercion, and Competition: The different pathways to policy convergence, University of Chicago, February 2004.
The most obvious disadvantage to this strategy is connected to the two latter features: a level playing field between the EU and the US does not necessarily reflect the preferences of the EU and may require it to lower its standards of protection.

The exercise of external powers by the EU has led to a few bilateral agreements with the US, facilitating the exchange of personal data between both jurisdictions, subject to compliance with data protection standards. These agreements cover the exchange between private parties, between private parties and government actors, as well as between government actors inter se.

The exchange of personal data between private parties was the object of the Safe Harbour agreement of 2000, which was declared invalid by the Court of Justice in the Schrems ruling of 6 October 2015. This agreement was based on practical considerations, in order to ensure that the flow of personal data from the EU to the US fulfils the requirements of Directive 95/46 on data protection. An important element of the agreement is the enforcement in the US, which was ensured by the Federal Trade Commission. The FTC had declared its strong commitment to vigilant Safe Harbour enforcement.

From the European side there was criticism of the agreement, in particular concerning the transparency, the enforcement and the access to data by US government authorities. This was a reason for the European side, as a consequence of the Snowden revelations, to seek a review of the agreement.

The exchange between private parties and government actors led to bilateral agreements aiming at reconciling privacy and security relating to the use and transfer of passenger name records (PNR) to the US Department of Homeland Security, and to the processing and transfer of financial messaging data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (TFTP). These agreements allow the access of US authorities to data from the private sector in the EU, subject to conditions related to data protection. Also

---

2495 Case C-362/14, Schrems, EU:C:2015:650
2496 See also Chapter 7, Section 5 of this study.
2498 COM(2013)847 - Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies.
2500 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ (2012) L 215/5. This agreement was preceded by two earlier agreements.
2501 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195/5.
in these cases, there is European concern regarding the implementation of the agreements. This is one of the reasons why the agreements envisage joint mechanisms for their review, focusing on implementation.

The exchange between government actors in the law enforcement sector is the (main) subject of the negotiations on the EU-US Data Protection and Privacy Agreement (“Umbrella Agreement”), which supplements existing agreements with only limited provisions on data protection, and aims to set minimum standards for data protection where personal data are exchanged between the law enforcement authorities in the two jurisdictions. The negotiations on this agreement started in March 2011 and have not been easy, also as a result of one recurring issue, the right of effective judicial redress to be granted by the US to EU citizens who are not resident in the US. In September 2015, the Commission announced that the negotiations had been finalised. The signature and the conclusion of the agreement now depend on the adoption of the Judicial Redress Bill by the US Congress, which must grant EU citizens judicial redress under the US Privacy Act of 1974.

The rationale of all these agreements with the US is to facilitate the transfer of personal data from the EU to the US. The agreements do not harmonise the level of protection between the EU and the US, nor do they use the concept of mutual recognition. The EU recognises the level of protection in the US, including the enforcement on the US side, but this recognition is not mutual. In this sense, the agreements are exponents of a mix between a unilateral and a bilateral strategy, not of a genuine bilateral strategy.

In short, a bilateral agreement on privacy and data protection between the EU and the US, as an example of a like-minded country, based on reciprocity, would be something new. An agreement does not necessarily mean an approximation of standards of privacy and data protection on both sides of the Atlantic Ocean, but could also focus on mutual recognition, standardisation processes or enforcement cooperation.

---


2504 E.g., Article 9 of the Agreement on mutual legal assistance between the European Union and the United States of America, which entered into force on 1 February 2010.


2509 As explained above in this section in relation to Safe Harbour.
14. **Multilateral Strategy: Towards Global Protection in the Framework of the UN**

The multilateral strategy aims at developing global standards, or, in other words, by pursuing this strategy, the European Union would operate as generator of global rules, which would most logically be enacted within the framework of the United Nations.

This strategy has three distinct justifications. First, the objective of influencing global governance based on EU values would be one of the main reasons for action, in view of the moral imperative under Articles 3(5) and 21 TEU. Diogenes’ citizen of the world deserves strong protection. Second, a reason for the European Union to pursue global rules on data protection would be to avoid the protection of individuals within the Union being compromised because of the fact that the rules in other parts of the world are more lenient. Third, economic reasons could provide a motivation, because global standards could contribute to creating a level playing field for economic actors.

Although, in the area of privacy and data protection, there is no global consensus on the values of protection and the ways to deliver protection, this multilateral strategy would not start from scratch. As confirmed by the United Nations High Commissioner for Human Rights: “International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data.” Furthermore, in the context of the UN online privacy is high on the agenda, although no concrete initiatives for a global agreement have yet been taken. On a more practical level, suggestions have been made for global standards. An example is known as the ‘Madrid Resolution’ on international privacy standards, adopted by the International Conference of Privacy and Data protection authorities in 2009.

The multilateral strategy is rather a long shot. There is absence of global consensus at an aspirational level, in particular, where this approach implies agreement with countries that do

---

2511 See Section 5 above.
2513 Bradford specifies this in an interesting way. Even where harmonisation takes place in the market (on a level aspired by the EU) it would make sense to pursue legally binding harmonisation, to “lock in” EU standards; Anu Bradford, “The Brussels Effect”, 2012 Northwestern University Law Review Vol. 107, No. 1, at 47.
2516 Adopted in 2009, by the 31st International Conference. See www.privacyconference2009.org
2517 These three obstacles are also, albeit with different wording, listed in: De Hert, P. and Papakonstantinou, V., “Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?”, A Journal of Law and Policy for the Information Society, vol. 9, no. 2, 2013, 271-324, at 315-322.
not share basic democratic values. Moreover, there are diverging views on the level of preferred legislative arrangements, with the transatlantic divide relating to supervisory arrangements as the obvious example. Divergence also exists as to the preferred legal instrument for global privacy and data protection. Should this be a multilateral treaty or a lighter instrument like, for instance, a UN model law?

Furthermore, the institutional cooperation in the area of privacy and data protection is incomplete. Various international organisations are active in this area, but – as Kuner explains – it is not evident which organisation should take the lead. The OECD is not an organisation that produces binding agreements, the Council of Europe may be regarded as being too European and specialised UN agencies such as UNCITRAL and UNIDROIT have not yet become involved in data protection.

In addition, one could question the legitimacy of the United Nations to set global rules on the fundamental rights of privacy and data protection. As such, the United Nations as a global organisation would qualify for taking the lead in this domain, if only because of its number of members. However, a large number of states within the United Nations do not share the essential democratic values of the European Union and the United States. As Mazower explains, objections against involvement of the United Nations are common in the United States, for a number of reasons, but also because non-Western/non-democratic countries have a large say on the policies of the United Nations.

**However, there are incentives for the EU to pursue the multilateral strategy**

The most important incentive for the European Union to pursue a multilateral strategy for privacy and data protection is probably the scale of the problem. The effect of technological developments such as big data or mass surveillance might – or better: should – create a sense of urgency to seek global solutions, as the most effective answer to global developments in the information society. This sense of urgency may even increase because of grown public awareness. The need to join forces might also result from considerations of cost effectiveness or scarce resources.

---


2520 Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013, at 163.

2521 The United Nations has 193 states as members (July 2015).

2522 The report by Freedom House on Freedom of the World 2014 mentions a number of 55% of the countries in the world (on a total of 185 included in report) considered not free, or only partly free, https://freedomhouse.org/report/freedom-world/freedom-world-2014.


2525 Financial resources of governments as well as the limited availability of highly qualified staff.
A multilateral, global agreement, possibly under the umbrella of the United Nations would – despite the objections mentioned above, for the long term in any event – be the most appropriate instrument of effectively ensuring privacy and data protection on a global scale. As observed above in relation to bilateral agreements, an agreement does not necessarily include an approximation of standards of privacy and data protection, but could also focus on mutual recognition, standardisation processes or enforcement cooperation.

Privacy and data protection are also connected to the global cooperation within the World Trade Organization, because of the fact that data protection rules regulate and even restrict transborder data flows. The General Agreement on Trade and Services liberalised the provision of services, but contains an exception for the rules necessary to ensure compliance with rules for the protection of privacy in relation to the processing and dissemination of personal data. This provision confirms that privacy and data protection should not be integrated into trade agreements nor into activities of the WTO, as an organisation whose task is to supervise and liberalise international trade, not to protect fundamental rights. At the same time, privacy and data protection as fundamental rights should not be negotiable in the context of a trade agreement. These arguments are used mostly in the European Union, also in relation to the Transatlantic Trade and Investment Partnership (TTIP), an agreement that is currently being negotiated between the EU and the US. Since the inclusion of privacy and data protection in trade agreements is a very controversial issue, it will not be further discussed here as a promising avenue for EU action on the international scene.

15. The Meaning of the Three Strategies for the CJEU: Google Spain as an Illustration of the Unilateral Strategy under Article 16 TFEU

The ruling in Schrems coincided in time with the finalisation of the research for this study. Clearly, Schrems can be seen as a typical illustration of a unilateral strategy of the European Union, if only because of the high requirement for adequacy of the protection in a third country, under Article 25 of Directive 95/46, which the Court of Justice understands as a level of protection that is essentially equivalent to the level guaranteed within the Union.

The ruling of the Court of Justice in Google Spain and Google Inc. is the second example of how the unilateral strategy is integrated in the case law of the Court of Justice. This ruling

---

2526 The WTO has 161 states as members (July 2015).
2527 Article XIV(c)(ii) GATS, available on: https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm
2529 Further read: Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013, at 163, at 52, and footnotes mentioned there.
2530 Case C-362/14, Schrems, EU:C:2015:650
2531 At 73 of the ruling.
2532 Case C-131/12, Google Spain and Google Inc., EU:C:2014:317
is the focus of this section, also because at time of writing the consequences of Schrems were still unclear.

In its ruling, the Court confirmed the wide external effect of European data protection law on the internet. It referred to the objective of ensuring effective and complete protection of fundamental rights and, in connection with this objective, to the particularly broad territorial scope of Directive 95/46. The Court declared expressis verbis that it “cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46”.

Hence, for the Court of Justice effectiveness of the protection of Europeans is the main reason to unilaterally accord a wide external effect of EU law in this area. This is in line with the claim in the Treaty on European Union that fundamental rights are universal.

However, the Court did not address the impact of its ruling on competing jurisdictions on the internet. This problem provoked a debate on the jurisdictional aspects of the Court’s ruling, revealing a number of sensitivities incited by the wide territorial scope of EU law on the internet, as interpreted by the Court of Justice. In this context, Kuner refers to the growing insularity of EU law. These sensitivities come from two seemingly opposite perspectives. On the one hand, there is the viewpoint that the application of EU law would potentially cover the entire internet, and thus directly interfere in other jurisdictions. On the other hand, it is argued that the effect of the ruling could be a fragmented internet, which would prejudice the benefits of the internet as a global network.

The implementation of the ruling by Google aims to address these two viewpoints, by deleting the links to individuals only from its European-directed search services (the domains relating to the EU Member States) and not from the generic domain ‘google.com’. This approach would not only ensure that the effect of the Court’s ruling would not be felt outside the territory of the European Union, but also that the generic domain of the internet would not be fragmented between jurisdictions. The argument against this approach is

---

2533 At 53-54 of the ruling.
2534 At 58 of the ruling.
2535 As expressed in the preamble and in Article 21 of the TEU.
2536 The sensitivities around the balance between privacy and data protection and freedom of expression are not addressed – not relating to jurisdiction – are addressed in Chapter 5.
2539 See on this Chapter 5, Sections 12 and 13 of this study.
2540 As a personal observation, this was discussed during a hearing organised by the Advisory Council to Google on the Right to be Forgotten, in Brussels on 4 November 2014. Whereas I insisted in a more effective implementation of the delisting required by the ruling, including Google.com, the reply by Google’s chief legal officer was that including google.com on a regional basis could also trigger requests from other – non-democratic – jurisdictions for deleting information from google.com when approached from within such jurisdictions, and could hence lead to censorship. See: The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015, at 5.4.
obvious: it would make it easy to circumvent the effectiveness of the ruling within the Union itself. This is why the Article 29 Working Party states that the de-listing must also be effective on Google.com, a viewpoint that is not shared by the Advisory Council to Google on the Right to be Forgotten. This resulted in an enforcement action by the French data protection authority, the CNIL, against Google.

The Advisory Council observes in this context that there may be “a competing interest on the part of users outside of Europe to access information via a name-based search in accordance with the laws of their country”. This observation challenges the result of the ruling that an EU court can limit the access to search results by a national of a third country whereas under his or her national law the access would be legal and possibly even a constitutional right. The question is whether this is problematic. The answer to this question is in our view negative. Effective data protection for Europeans necessarily may mean a limitation of access by individuals in third countries, resulting from a need to avoid circumvention of the effective right to data protection. Since Google Spain and Google Inc. only applies to personal data of Europeans, it is submitted that this judgement does not substantially affect fundamental rights of individuals to receive information, in third countries.

The observation shows that applying a unilateral strategy by the Court of Justice requires that there must be a meaningful link with the European Union, and a link is indeed required by the Court. In Google Spain and Google Inc. extraterritorial application of EU law was based on the need for protection of individuals within the scope of the Charter. Moreover, in Lindqvist the Court ruled that the entire internet cannot be made subject to EU data protection law. However, the case law is not (yet) clear about the precise nature of this link.

How would the CJEU deal with bilateral and multilateral strategies?

The ruling in Schrems on the Safe Harbour Agreement between the EU and the US has been the first opportunity for the Court of Justice to rule on the compatibility of agreements of the European Union with third countries and international organisations on privacy and data protection with EU law. The Court annulled the Safe Harbour Agreement. The second
opportunity will be the opinion on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of passenger name record data, as requested by the European Parliament.

In view of these two cases, it is to be expected that the Court will provide more clarity on the essential requirements for bilateral and multilateral agreements that affect the protection of individuals within the European Union, building on its first assessment in Schrems. These requirements could be based on the presumption that effective protection is also needed outside the EU territory, but that it may probably not be fully similar to the protection offered within the EU territory, because enforcement is more complicated and because account has to be taken of diverging legal systems outside the EU territory and their legitimate claims of jurisdiction. The notion of adequacy of the level of protection of data transfers under Article 25 of Directive 95/46 could serve as an inspiration. In Schrems, the Court explained adequacy as meaning essential equivalence.

Possibly, Article 52(1) Charter and, in particular, the obligation to respect the essence of rights and freedoms would be a good benchmark in the external context and could set a relevant minimum standard. Article 52(1) Charter could also provide an indication of the conditions that would allow for mutual recognition (or: interoperability) of systems. We also recall the general case law of the Court of Justice on the protection on fundamental rights, particularly Kadi and Al Barakaat, which specified that the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty and in particular the fundamental rights. Finally, the enforceability of the rights to data protection of individuals in the European Union is a consideration. In Digital Rights Ireland and Seitlinger the Court emphasised the control, required explicitly by Article 8(3) Charter, by an independent DPA, as an essential element of data protection that could be prejudiced where personal data are not retained within the European Union.

16. The Meaning of the Three Strategies for the EU legislator: Giving Wide External Effect with the Unilateral Strategy as a Composing Element

The EU legislator gives wide external effect: the unilateral strategy plays a key role

The unilateral strategy in the external domain plays a key role in Directive 95/46 on data protection. The EU legislator did not rely on the general rules on jurisdiction, but provided for a specific jurisdictional regime, which is not common in data protection law in third countries. The directive acknowledges the need for a wide jurisdiction in its Article

2549 Opinion 1/15 on Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (pending).
2550 Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461, at 282-285 discussed in Chapter 2, Section 5 of this study.
2551 Joined cases Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 68.
2552 Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law, Ex Tuto Publishing 2013, at 89.
4(1)(c), based on the notion that an individual must also be protected when the processing of data is carried out by a person established in a third country.\textsuperscript{2553} This is what the Court of Justice identified as a “particularly broad territorial scope”.\textsuperscript{2554} The perspective adopted by the legislator was the use of equipment, automated or otherwise, situated on EU territory. This led to a lively practice, in which the Article 29 Working Party, for instance, advised that the installation of cookies on computers of users in the European Union would trigger the applicability of the directive.\textsuperscript{2555}

The proposed General Data Protection Regulation widens the applicability further to the processing activities “related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour”.\textsuperscript{2556}

This wide external effect is not only given to provisions laying down a wide territorial scope of EU data protection law,\textsuperscript{2557} but also to the provisions on transfers of personal data to third countries and international organisations.\textsuperscript{2558} The requirement of adequacy of the level of protection afforded by a third country as the main ground for allowing transfer is a perfect example of how internal EU law can have wide external effect.

\textit{The regime of data transfers: a typical example of a unilateral strategy}

The adequacy regime for data transfers under Article 25 of Directive 95/46 on data protection is a typical example of the unilateral approach. The European Union accepts the transfer of data to third countries who adhere to the European standards, although some leeway is given to these third countries. Their level of protection must not be the same as that of the Union itself. An adequate level is sufficient.\textsuperscript{2559} In a guidance paper of 1998, the Article 29 Working Party understands this as encompassing a core of data protection principles and effective means for their application\textsuperscript{2560} that does not necessarily have to be equal to the level of the European Union and does not require that the country of destination has established an independent data protection authority.\textsuperscript{2561} Arguably, this last point is outdated since the

\begin{footnotesize}
\begin{enumerate}
\item Recital (20) of Directive 95/46.
\item Case C-131/12, \textit{Google Spain and Google Inc.}, EU:C:2014:317, at 54.
\item Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, WP 179, at 21-22.
\item In particular in Article 4(1)(c) of Directive 95/46 and in Article 3(2) of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
\item Article 12(3)(a) of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 requires an equivalent level.
\end{enumerate}
\end{footnotesize}
Treaties now confirm independent control as a core element of data protection, in Article 16(2) TFEU an Article 8(3) Charter. In Digital Rights Ireland and Seitlinger the Court of Justice emphasised the need for effective control. More in general, the leeway for third countries seems to be restricted in Schrems, to the extent the Court explained adequacy as essential equivalence.

In any event, the European Union unilaterally decides the level of protection that is required for a transfer of data. Article 26 of Directive 95/46 contains derogations, but the application of these derogations is unilaterally decided by the Union and its Member States. The proposed General Data Protection Regulation maintains and further refines this system. The system will be reinforced and simplified, in view of the challenges of globalisation. Particularly, the tool of Binding Corporate Rules will be streamlined and extended. This will not change the unilateral nature of the system.

The importance of transfer as an element of the unilateral strategy has increased due to the developing information society, where the availability of personal data outside the European Union may already be qualified as a transfer, for instance in a cloud environment. Transfer within the meaning of EU data protection law is an important element of transborder data flows, and is a global phenomenon that the EU side has regulated by applying its own standards. The Court of Justice interpreted the notion of transfers under Directive 95/46 in Lindqvist.

**Article 43a of the proposed GDPR, a unilateral solution for a conflict of law**

Article 43a of the General Data Protection Regulation, which was suggested by the European Parliament, addresses a situation where the systems of the European Union and third countries are incompatible, and where no mutual legal assistance treaty or international agreement is in force providing for a solution for the incompatibility. This provision is entitled “transfers or disclosures not authorised by Union law”. The European Parliament's suggestion provided a prohibition for controllers or processors of EU data from disclosing personal data to third-country administrative or judicial authorities.

---

2562 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, at 68.
2563 Case C-362/14, Schrems, EU:C:2015:650.
2566 European Data Protection Supervisor, Opinion of 26 November 2012 on the Commission’s Communication on "Unleashing the potential of Cloud Computing in Europe", at 72-76.
2567 Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013, at 163, at 159-160.
2568 Case C-101/01, Lindqvist, EU:C:2003:596, at 58 and 69. See Section 10 above.
unless a prior authorisation of the competent DPA has been obtained. This DPA role was not accepted by the other institutions, but other elements are included in the outcome of the trilogues. The provision deals with possible requests from third states’ governments that may breach EU data protection law and is a reaction to the Snowden revelations, as far as access by the NSA to personal data of EU citizens stored by US internet companies is concerned under the PRISM programme.

The provision envisages protecting the individuals in the European Union, where internet companies are under a legal obligation in a third country that implies a breach of EU data protection law. This provision is a unilateral instrument and does not recognise claims by third countries under their national laws. The effect of the provision could be to encourage third countries to enter into negotiations with the Union to solve the conflict of law.

The bilateral and multilateral strategies: external action by the EU legislator on privacy and data protection as a promising avenue, not necessarily harmonising the level of protection

This chapter mentioned agreements with the United States and also discussed the roles of the United Nations, the OECD and the Council of Europe, in relation to the European Union. External EU action by the EU legislator is a promising avenue precisely because of the global nature of the phenomena under discussion, which should be further explored. A distinction must be made between bilateral agreements with certain third countries and multilateral agreements.

The scope of external EU action is determined by the powers conferred on the European Union under EU law, and subsequently by the way these powers are exercised. As explained above, an agreement does not necessarily include an approximation of standards of privacy and data protection, but could also focus on mutual recognition, standardisation processes or enforcement cooperation. As an illustration, one subject may be mentioned that would qualify for inclusion in an agreement, the concept of accountability. As was explained in Chapter 6, this concept is as a modern instrument of ensuring data protection and has a prominent place in the OECD Guidelines on the Protection of Privacy and Transborder Flows.

---

2570 This provision is not included in the documents of the Commission and of the Council. The EDPS proposes a softer version of this provision, European Data Protection Supervisor, Opinion of 27 July 2015 - Europe’s big opportunity, EDPS recommendations on the EU’s options for data protection reform, and the Annex - Comparative table of GDPR texts with EDPS recommendations.
2572 Planning Tool for Resource Integration, Synchronisation and Management (PRISM) of the NSA, See Chapter 3, Sections 7 and 8.
2573 This is not necessarily the effect. The provision could also intensify the controversy between the EU and the US, what Bygrave calls the Transatlantic Privacy Divide, Lee A. Bygrave, Data Privacy Law, An International Perspective, Oxford University Press 2014, at 107-116.
2574 In Section 4.
2575 Here agreements are meant in a wide sense, including international treaties, but also more informal tools for international cooperation.
2576 Further read, Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press 2013, at 163, at 175-180.
of Personal Data (1980), as amended on 11 July 2013,\textsuperscript{2577} as an obligation for data controllers to put a privacy management programme in place.\textsuperscript{2578}

Accountability is a flexible instrument that should be tailored to “the structure, scale, volume and sensitivity of operations”.\textsuperscript{2579} Due to this flexibility, accountability is also an arrangement that could be included in agreements with third countries and with international organisations, without necessarily harmonising data protection standards. Accountability could be tailored to the specific characteristics of the jurisdiction in which an accountable organisation operates and could ensure compliance with different requirements depending on the jurisdiction.\textsuperscript{2580} Binding Corporate Rules, included in the proposed General Data Protection Regulation,\textsuperscript{2581} are a specific expression of accountability.\textsuperscript{2582}

In any event, promising bilateral or multilateral strategies include ways of ensuring the interoperability between different legal systems, without necessarily requiring that the level of protection in other regions of the world is adapted to the EU level, nor that the level of protection in the European Union must be lowered.

17. **The Meaning of the Three Strategies for the DPAs and the Cooperation between them: Extending Cooperation to Authorities in Third Countries**

As was explained in Chapters 7 and 8, control is an essential element of data protection and cooperation between DPAs is an essential element of control.\textsuperscript{2583} The cooperation mechanisms of DPAs are essential in the external domain, in view of the global scale of the problem.

*Regulators and external action: the basis is a unilateral strategy, ensuring the control of EU law*

Control of the compliance with EU data protection law in an internet environment includes enforcement vis-à-vis data controllers who have their headquarters or their processing activities in a third country. This is a substantial part of the task of the DPAs, resulting from the fact that big internet companies have their headquarters outside the European Union. It is also complicated, as may be illustrated by the difficulties of regaining control over the

\textsuperscript{2577} C(2013)79, published on website OECD.
\textsuperscript{2578} Guideline 15.
\textsuperscript{2579} Guideline 15, a) ii.
\textsuperscript{2581} Article 43 of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
\textsuperscript{2582} Lee A. Bygrave, Data Privacy Law, An International Perspective, Oxford University Press 2014, at 209.
\textsuperscript{2583} E.g., in Chapter 8, Section 1.
privacy settings of big internet companies through enforcement by DPAs. These difficulties triggered this study.2584

In its essence, the task of DPAs (and of cooperation mechanisms of DPAs) of ensuring control is a unilateral task, ensuring that individuals are protected in accordance with European and national law applicable within their respective jurisdictions. As was explained in Chapter 8, the task of DPAs also involves contributing to the protection of individuals all over the Union.2585 The task also has extraterritorial components outside the European Union, including the use of enforcement powers in an external context.

This being said, the basis of the work of the DPAs in their policy activities and their enforcement practice is defending the high European standards, not aiming at finding compromises with lower standards of third countries. There is no evidence that the practice is different.

The cooperation between DPAs and regulatory agencies in third countries as an exponent of the bilateral and multilateral strategy

Fulfilment of the task of DPAs is not only a unilateral activity. Fulfilment of this task also requires cooperation with authorities in third countries, including cooperation with regulatory authorities in third countries, in order to ensure effective control. The cooperation between DPAs and regulatory agencies in third countries has been developing over the last years, in a bilateral as well as a multilateral context.

This cooperation can be qualified as policy cooperation, where DPAs cooperate in order to create a better understanding of privacy and data protection issues or where they engage in common policy development. An important mechanism in this type of cooperation is the International Conference of Privacy and Data Protection Authorities, which presents itself as “the assembly of all accredited data protection and privacy commissioners from around the world”.2586 Under its rules and procedures the Conference is an entity in its own right, representing its members and one of its purposes is to promote and enhance personal data protection and privacy rights at the international level.2587 This conference adopts resolutions and declarations.2588 In 2009 it adopted the Madrid Resolution with a proposal for international privacy standards.2589 It would be in line with the principle of sincere cooperation, as explained above, for the DPAs within the European Union to inform the EU institutions of the positions they are taking in such fora, to the extent these positions may affect the consistency of EU policies. This could be a role for the Chair of the Article 29 Working Party.

2584 See Chapter 1, Section 1 of this study.
2585 As explicitly recognised in Article 46(1) of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
2586 https://www.privacyconference2015.org/the-international-conference/
2588 https://www.privacyconference2015.org/resolutions-declarations/
2589 Adopted by the 31st International Conference of Privacy and Data Protection Authorities (2009).
Another type of cooperation is to engage in enforcement cooperation. Examples of bilateral enforcement cooperation can be found in the cooperation of various DPAs in the European Union with the Federal Trade Commission, as illustrated in memoranda of understanding concluded between the FTC respectively with the DPAs in Ireland, the United Kingdom and the Netherlands. These MOUs include intentions to share information, provide assistance in investigations and to coordinate enforcement actions.

An example of multilateral cooperation is the Global Privacy Enforcement Network ("GPEN"), facilitated by the OECD, in the context of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, recommending, for instance, to improve domestic frameworks for privacy law enforcement, to better enable authorities to cooperate with foreign authorities and to develop effective international mechanisms to facilitate cross-border privacy law enforcement cooperation and to provide mutual assistance to one another.

Bilateral and multilateral cooperation on enforcement is essential for ensuring effectiveness of control in an internet environment. However, it also raises questions of legitimacy since arrangements on enforcement also mean sharing responsibility with authorities in third countries. These arrangements are an additional element to the composite administrative network within the European Union where responsibilities are shared. This requires precise rules on responsibilities, ensuring access to justice under the rule of law (judicial accountability) and a transparent regime of reporting in order to enhance the democratic accountability. Inspiration could be drawn from Point 25 of the Joint Statement and Common Approach of the European Parliament, the Council of the European Union and the European Commission on Decentralised Agencies, which envisages the streamlining of external activities of EU agencies, for instance through dedicated work programmes and by laying down principles and modalities for international cooperation. A specific element of these precise rules could be rules on the exchange of personal data between these authorities.

Whereas the proposed General Data Protection Regulation includes precise rules on the cooperation of DPAs and on consistency, it remains general on the enforcement cooperation with authorities of third countries and with international organisations. This is an omission that should be addressed.

---

2593 See: https://www.privacyenforcement.net See also section 5 above.
2595 This was explained in Chapter 8, Section 7.
2596 Chapter VII of the proposal.
18. Conclusions

This chapter discussed the external aspects of Article 16 TFEU, focusing on the relations with third countries and international organisations. On the internet, protection of EU citizens does not stop at the external borders of the European Union, but has an inherent external effect. Giving extraterritorial effect to EU data protection law is also an explicit objective of the EU legislator, resulting from the general ambitions of the European Union to promote its essential values, also in the wider world.

As a rule, any intervention by the European Union with the purpose of ensuring privacy and data protection on the internet has extraterritorial effect. Giving extraterritorial effect to EU data protection law is an explicit objective of the EU legislator. The horizontal relationship between the European Union and jurisdictions of third countries is one of the main complicating factors of effective internet regulation. Another complicating factor is the vertical relationship between the Union and international organisations that are active in the area. (Section 2)

From an institutional perspective, the qualification of DPAs as new branches of government has institutional consequences in the external domain. In the areas of their competence, the DPAs represent the European Union externally. However, they must respect the consistency of external EU policy. The principle of sincere cooperation binds the DPAs, but also obliges the EU institutions to involve the DPAs where they take positions in the external domain on policies concerning privacy and data protection, for instance in negotiations with third countries in this area, conducted according to the procedure of Article 218 TFEU. DPAs should not commit the Union to international obligations, but are empowered to enter into enforcement arrangements. (Section 3)

In the external relations with third countries, the relationship with the United States plays an important role. An important element of the controversy between the EU and the US is a difference in approach between the two jurisdictions. The approach of the US – at least in relation to consumer privacy – does not aim at giving wide territorial scope to US law, but at increasing interoperability in privacy laws by pursuing mutual recognition. In contrast, the nature of privacy and data protection as fundamental rights under EU law prevents the mutual recognition of substantive principles of EU law in this area, if the standards in a third country do not comply with the Charter. (Section 4)

Two of the most relevant international organisations for the EU are the UN and the OECD. Under current law the UN does not impose any obligation on the EU in the field of data protection. However, the EU should encourage the UN to play a more prominent role. The OECD guidelines emphasise the need for improved interoperability of privacy frameworks and for cross-border cooperation between privacy enforcement authorities. The OECD is a suitable forum for discussion with the US. (Section 5)
The closest ally of the European Union is the Council of Europe, which provides inspiration for EU privacy and data protection, through the case law of the European Court of Human Rights and through Convention 108. Institutionally, it is a difficult relationship, as illustrated by the negative Opinion of the Court of Justice on the draft accession agreement of the Union to the ECHR, referred to in Article 6 TEU. An example in the domain of privacy and data protection illustrates the difficult relationship: ratification by a third country of Convention 108 – meaning compliance with the Convention – does not guarantee that the level of protection provided by a third country is considered adequate under Directive 95/46 making it possible that personal data are transferred to this third country without further safeguards. (Section 6)

The European Union itself is an organisation sui generis, also in the international domain. International competence of the Union, under international law, is similar but not equal to a state. The Union is not a member of international organisations such as the UN, the OECD and the Council of Europe. Under Article 16 TFEU, an exclusive external EU competence must be assumed because effective protection on the internet requires the widest possible geographical scope. Arguably, the Member States have lost their external competence in the domain of privacy and data protection. In any event, the Member States are expected to lose their competence after the entry into force of the GDPR, at least in the areas covered by this instrument. (Section 7)

Where the European Union uses its external competence, it acts under international law. The Court of Justice determines the limits of external competence and, in certain circumstances, of the primacy of international law. It is the Court itself that ultimately – and in last resort exclusively – interprets the Charter and, more generally, EU law. Provisions of international agreements have direct effect within the EU legal order, but subject to the nuance that international law cannot have the effect of prejudicing the constitutional principles of the Treaties (the Kadi case law). (Section 8)

The overlapping of jurisdictions on the internet is no longer an exception. Under public international law, there is no generally accepted solution for internet jurisdiction. General public international law implies that states – and the European Union – are precluded from enforcing their laws in another state’s territory, but they may prescribe rules for persons and events outside their borders. In accordance with public international law, the European Union – acting as a state – should claim extraterritorial jurisdiction, even in the absence of enforcement power, for instance to stimulate voluntary compliance in third countries. Due to the pervasiveness of the internet in our daily lives, the internet should not be governed by a separate body of law. (Section 9)

If external EU jurisdiction in the area of privacy and data protection is to be claimed legitimately, that claim should be based on a meaningful link with the effective protection of the individual in the European Union. This meaningful link with the Union could consist of personal jurisdiction based on residence and the doctrine of effect. The study suggests that the Union should promote this foundation of personal jurisdiction in the international context.
This suggestion does not aim at solving the problem of internet jurisdiction, but it could be included in the external EU action in the area of privacy and data protection. (Section 10)

The European Union emphasises the need for taking responsibility for globalisation, claiming that its values have a normative strength and that they are universally applicable. The Union has global power through the legal standards representing these values. On this basis, the study distinguishes three strategies for the Union operating in the external domain: a unilateral, a bilateral and a multilateral strategy. This does not exclude that in practice a smart mix of the three previous strategies would be the best option. (Section 11)

The unilateral strategy basically means exporting the EU standards. This is a potentially successful approach, on the basis of the conditions of Bradford summarised as the “Brussels effect”. The European Union has regulatory clout, manages to set the global standards for regulation on privacy and data protection, is capable of exporting its system on privacy and data protection, and of assuming leadership in global regulation. The Union could use facilities offered by the Council of Europe, such as the possibility that non-European countries adhere to Convention 108. On a practical level, this strategy allows bridges to be built with like-minded countries, finding communalities for joint challenges relating to internet privacy. (Section 12)

The bilateral strategy involves seeking for arrangements with relevant, like-minded jurisdictions such as the US and, by doing so, building bridges between these jurisdictions. A bilateral agreement on privacy and data protection between the EU and the US, based on reciprocity, would be something new. An agreement does not necessarily mean an approximation of standards of privacy and data protection, which could be difficult to reconcile with the Charter, but could also focus on mutual recognition, standardisation processes or enforcement cooperation. (Section 13)

The multilateral strategy aims at developing global standards. The European Union should strive for global rules, most logically within the framework of the United Nations. The multilateral strategy is rather a long shot, but a multilateral, global agreement, would in the long term be the most appropriate instrument to effectively ensure privacy and data protection on a global scale. Such an agreement does not necessarily include an approximation of standards, but could also focus on mutual recognition, standardisation processes or enforcement cooperation. (Section 14)

The Court of Justice contributed, in Google Spain and Google Inc., to the unilateral strategy under Article 16 TFEU, by highlighting the effectiveness of the protection of Europeans and by requiring a meaningful link with the European Union. The Court did not address the impact of its ruling on competing jurisdictions on the internet. The ruling in Schrems2597 on the Safe Harbour Agreement with the US2598 was the first opportunity for the Court to clarify

---

2597 Case C-362/14, Schrems, ECLI:EU:C:2015:650.
the essential requirements for bilateral and multilateral agreements, affecting the protection of individuals within the Union. A second opportunity will present itself with the Opinion on the agreement with Canada on passenger name record data.2599 (Section 15)

The EU legislator gives wide external effect to EU law on data protection, with the unilateral approach as a composing element and with the regime of data transfers as typical example. Article 43a of the proposed General Data Protection Regulation is a unilateral solution for a conflict of law. Promising bilateral or multilateral strategies include methods to ensure the interoperability between different legal systems, without necessarily adapting the level of protection in other regions of the world to the EU level, or lowering the level of protection in the European Union. Accountability of data controllers and processors could be included in international agreements. (Section 16)

For the DPAs and the cooperation between DPAs the starting point is a unilateral strategy: their task is to control the application of EU law. The cooperation between DPAs and regulatory agencies in third countries is an exponent of the bilateral and multilateral strategy. Bilateral Memoranda of Understanding between European DPAs and the Federal Trade Commission and multilateral cooperation in the Global Privacy Enforcement Network are examples. The proposed GDPR should have included rules on enforcement cooperation with authorities of third countries and with international organisations. (Section 17)

In the external domain, the European Union should also respect some degree of accountability towards political institutions. This accountability is related to the democratically agreed substantive level of privacy and protection, as laid down in the EU rules under Article 16(2) TFEU. Where the Union acts in the external domain, individuals may have the legitimate expectation that this does not lower the level of protection of individuals in the Union.

The three strategies (i.e. the unilateral, bilateral and multilateral strategies) should deal with the two types of issues mentioned earlier: conflicting jurisdictional claims and divergences in substantive law. Reconciling legitimacy and effectiveness in relation to jurisdictional claims means: ensuring effective protection of individuals in the European Union and, at the same time, basing the legitimate claim of jurisdiction on the internet on a meaningful link with the Union. Divergences in substantive laws could be addressed by allowing practical arrangements with third countries and international organisations on an effective level of protection, but not by lowering the legitimate level of protection of individuals in the Union.

In order to ensure effective protection of individuals on the internet, the preferred strategy should be the unilateral strategy, aiming at exporting EU values in the international domain. In addition, the bilateral strategy should be explored, possibly under the wings of the OECD and focusing on mutual recognition, standardisation processes or enforcement cooperation, based on the communalities between the systems, but also accepting the differences. In the

2599 Opinion 1/15 (pending) on Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data
long term, a UN Treaty would ensure the best protection (the multilateral approach). The European Union should take initiatives in order to facilitate the adoption of such a Treaty, with the ambition to achieve a minimum standard of data protection.
Chapter 10. Making Article 16 TFEU Work: Analysis, Conclusions and an Analytical Grid

1. Introduction

The European Union acts, under Article 16 TFEU, as a constitutional guardian of privacy and data protection. In an information society, the fundamental rights of privacy and data protection remain essential values for our democracies that are subject to the rule of law. However, at the same time, this information society is challenging the enjoyment of these fundamental rights, with big data and mass surveillance as the most obvious illustrations.

This study started with the Snowden revelations and with the difficulty for governments to gain control over the privacy policies of search engines and social networking providers, as may be illustrated by the complicated enforcement actions of data protection authorities vis-à-vis, particularly, Google and Facebook. The study also emphasised the resilience of the fundamental rights’ protection under the rule of law in the Union, as illustrated by the Court of Justice of the European Union in its recent ruling in *Schrems*. These cases are exemplary for the mass scale of data processing and for a lack of overview within democratic bodies and oversight bodies on what is actually happening, and how to keep control.

The mandate of the European Union under Article 16 TFEU was the subject of this study. This study analysed the role of the European Union in the field of internet privacy and data protection. The study focused on the contributions of the specific actors and roles within the EU framework: the judiciary, the EU legislator, the independent supervisory authorities, the cooperation mechanisms of these authorities, as well as the Union as actor in the external domain. This analysis showed that EU powers under Article 16 TFEU can be successfully used, in conformity with the requirements of legitimacy and effectiveness. It also showed that ambitious approaches are needed, in view of the huge challenges in the information society. The preceding chapters provided the elements for answering the research question:

How does the constitutional mandate under Article 16 TFEU contribute to legitimate and effective privacy and data protection on the internet and what does and should the European Union do to make Article 16 TFEU work, through judicial review, legislation and control by (cooperating) independent authorities, taking into account that the mandate has external effect?

This final chapter summarises and analyses the main findings of this study, and brings the different elements of the research question together, with the support of an analytical grid. The first objective of the chapter is to provide this analytical grid, which is intended to enhance the understanding of the mandate of the European Union and of the different roles within this mandate. The second objective is to analyse the findings in the previous chapters.

---

2600 *Case C-362/14, Schrems*, ECLI:EU:C:2015:650.
of this study – using the analytical grid – and to provide recommendations for a successful exercise of the mandate.

Section 2 recalls the main challenges and the outline of the governance of privacy and data protection under Article 16 TFEU, whereas Section 3 introduces the analytical grid that structures this chapter.

Sections 4-9 of this chapter analyse the conclusions of the corresponding Chapters 4-9 on the basis of the analytical grid. This means in concrete terms:

a. What is the substance of Article 16 TFEU and of the roles identified pursuant to this provision?

b. Which constitutional safeguards are imposed by EU law?

c. To what extent does Article 16 TFEU or the roles based on this provision enhance the legitimacy of the European Union in this domain?

d. To what extent does Article 16 TFEU or the roles based on this provision enhance the effectiveness of the European Union in this domain?

Section 4 is of a more general nature and will focus on the contribution of Article 16 TFEU to legitimate and effective privacy and data protection on the internet. Sections 5-9 analyse what the European Union does and should do, through the contributions of the various roles. Section 5 considers the role of the EU Court of Justice, which is ultimately responsible for ensuring that everyone’s right to data protection is respected; Section 6 focuses on the European Parliament and the Council acting as the EU legislator; Section 7 deals with the independent data protection authorities (DPAs), which must ensure the control; Section 8 explains the cooperation mechanisms of these authorities, which are not mentioned in Article 16 TFEU, but are an essential element of the control; Section 9 clarifies the role of the European Union in the external domain.

Section 10 is different in character and introduces the prospect of the General Data Protection Regulation. Once it has entered into force, this regulation will provide a further framework, enabling the Union to become even more successful. Section 11 contains final conclusions, taking an optimistic perspective. It ends with the analytical grid, summarising main findings of the study.

2. **General Design of Article 16 TFEU: Recalling the Main Challenges and the Outline of the Governance under this Provision**

The present section recalls the background, starting from the presumption that privacy and data protection are fundamental rights that matter on the internet. However, these rights are at risk. The stakes for the European Union in ensuring privacy and data protection are high. The section also refers to the main elements of the governance model under Article 16 TFEU.
The values of privacy and data protection and the qualitative changes in the information society

Our society is developing and individual behaviour is changing, also with regard to the collection, sharing and use of personal information. Many individuals share large amounts of personal data on the internet, on a voluntary basis. However, these developments and changes do not alter the fact that privacy and data protection are fundamental rights that deserve to be protected in our democratic societies, subject to the rule of law. EU law has confirmed the essential nature of privacy and data protection at the constitutional level, in particular in Article 16 TFEU and in Articles 7 and 8 Charter, which distinguish privacy and data protection as two fundamental rights.

This study argued that, in the information society, the distinction between the rights to privacy and data protection is becoming meaningless. Both fundamental rights are part of one system, since on the internet all processing of personal data potentially affects privacy. Moreover, the right to data protection is a right that is based on fairness. Individuals may expect that their personal data are processed fairly, but the right to data protection is not a right prohibiting the processing. A general right to prohibit data processing would, to say the least, be difficult to enforce, in view of the massive amounts of data processed in the internet environment.

The internet economy and the developments of communications on the internet have led to a qualitative change in relation to privacy and data protection. Our economy is driven by the use of large amounts of data, including personal data, and individuals profit from the benefits the information society brings them. The information society increases efficiency, leads to more opportunities and innovation, and is even said to improve the quality of our lives. Under these circumstances, privacy and data protection are increasingly under pressure. This study explained this tendency. The study focused on the internet as a networked society with a loose government structure. Big data enables unprecedented predictions on private lives and shifts powers to those who hold information and those who supply it. Mass surveillance is characterised by secrecy, which complicates democratic and judicial oversight and – at least potentially – has an impact on the behaviour of individuals. The qualitative change was summarised in various places of this study as a perceived ‘loss of control’.

This qualitative change justifies the analysis of the mandate of the European Union under Article 16 TFEU in the light of the developments in the information society and, on that basis, to provide recommendations for a successful exercise of the mandate, in the context of the internet. Of course, the mandate under Article 16 TFEU is broader and also applies to privacy and data protection in situations that are not related to the internet, where people are not connected through networks. However, these situations are losing, relatively speaking, importance and, thus, are also becoming less relevant for understanding Article 16 TFEU.

2601 This is also in line with the CJEU case law; see mainly the conclusions of Chapter 2.
Article 16 TFEU as an adequate mandate guaranteeing the privacy and data protection of EU citizens on the internet: the stakes are high

This study analysed the mandate of the European Union to guarantee the privacy and data protection of Europeans citizens on the internet. This analysis comprised the adequacy of the mandate as such and the way in which the Union – and the various actors and roles under Article 16 TFEU – uses and should use this mandate. The introduction of this study (Chapter 1) formulated three objectives for the exercise of the mandate. We repeat these objectives here:

a. Ensuring protection, through full respect of the rights to privacy and data protection and the restrictive application of exceptions and limitations.
b. Balancing with other fundamental rights and essential interests in society.
c. Managing centralisation, an inherent effect of the mandate of the Union under Article 16 TFEU, and includes balancing the mandate with the competences of the Member States.

The stakes are high. The study took the view that our democracies cannot function without privacy and data protection. These fundamental rights are an expression of human dignity and the autonomy of the individual. The two convincing arguments for privacy and data protection were: first, the world is not divided into good people who have nothing to hide and bad people who are monitored for a reason, and, second, constant monitoring changes peoples’ behaviour.

The developments in the information society challenge the protection of these fundamental rights in what some consider an unprecedented manner. The era of big data and mass surveillance by governments and big internet companies underscore this challenge.

This situation is perceived as a loss of control, where the European Union and the Member States do not provide sufficiently protection, also because the internet is a global structure and privacy and data protection are challenged by acts of governments and private companies located outside the European Union. Others speak about the data protection credibility crisis.

The stakes are high for a further reason. Article 16 TFEU contains a commitment for the Union to ensure privacy and data protection for all individuals within the European Union. The Union must honour this commitment, for two reasons. First, people are entitled to protection of these essential values and, second, the Union should be credible.

---

2603 See Chapter 1, Section 4.
2604 As explained in Chapter 2.
Privacy and data protection are fields where the Treaty legislator has provided the instruments for the Union to make the difference. Article 16 TFEU has the potential to become a success story for the European Union. The realisation of this potential depends on the contributions of the actors and roles under Article 16 TFEU.

Many of the challenges are of a global nature. Within the structure of the European integration, the European Union is the most appropriate platform to deal with these challenges. EU action in this domain complies with the principle of subsidiarity, one of the key principles for EU intervention. This does not mean that the European Union does or should do everything. The Member States and their authorities remain important players, also to ensure the legitimacy of interventions in this field, which affect the daily lives of the individuals.

As said, the stakes are high. Regaining control requires an ambitious approach. Article 16 TFEU enables the European Union to be ambitious, to deal with the challenges in the information society and to effectively ensure privacy and data protection in an internet environment. The ambitious approach is needed even more in the light of a more general phenomenon that has arisen in recent times: a declining role of nation-states and of government intervention, with a growing dependency of governments on cooperation with the private sector. The loose governance structures of the internet are exemplary for this declining role.

The governance model under Article 16 TFEU

Article 16 TFEU contains a specific mandate for the European Union in the domain of the protection of fundamental rights: an assignment for the Union to ensure protection. Under Article 16 TFEU, the Union must ensure everyone’s right to data protection.

This mandate has a wider scope than the Charter, which obliges the European Union – and the Member States acting within the scope of EU law – to respect the fundamental rights in their laws and policies. Article 16 TFEU implies an obligation for the Union to act and to ensure that citizens are protected. This obligation goes beyond the obligation to respect the fundamental rights in the course of interventions of the Union in other domains. Article 16 TFEU brings privacy and data protection by definition within the scope of EU law.

Article 16 TFEU also contains a governance model for privacy and data protection. This governance model provides for explicit roles for three (categories of) actors: the Court of Justice ensures that the rights to privacy and data protection are respected under the rule of law, the European Parliament and the Council acting as EU legislator adopt the rules and the independent data protection authorities ensure control. Within the structure of the European Union, based on an institutional balance and a separation of powers, the roles of these

---

2608 See, e.g., Conclusions Chapter 3.
2609 As interpreted by the CJEU in Case C-617/10, Åkerberg Fransson, EU:C:2013:280.
(categories of) actors are separate, not shared. The actors contribute to the fulfilment of the same mandate, but their responsibilities are separate. The qualification of the independent data protection authorities as new branches of government – in Chapter 7 of this study – illustrated this separation of responsibilities.

In an internet environment, this governance model of EU privacy and data protection also implies a role for cooperation structures of independent data protection authorities. The governance model further implies an active role of the Union as such in the international domain, in view of the global nature of the challenges for privacy and data protection.

The model further requires the involvement of other governmental and non-governmental stakeholders, not explicitly referred to in Article 16 TFEU. As this study demonstrated, involvement of other stakeholders is a success factor for the exercise of the EU mandate in an effective and legitimate manner, particularly in an internet environment.

In short, the governance model involves roles for institutions and bodies of the European Union, Member States, national DPAs, cooperation mechanisms of DPAs, private companies and representatives of the private sector, civil society as represented by NGOs, as well as third countries and international organisations. This governance model takes on different shapes, and resembles what is known in the literature as a composite administration, a multi-level governance or a multi-stakeholder model.

In many situations, not governed by the separation of powers, governance is shared between different actors, not separated. However, this sharing does not mean sharing the final responsibility. The involvement of other governmental and non-governmental stakeholders should not result in a situation in which the European Union can no longer assume its final responsibility for privacy and data protection. The EU should remain in the driving seat.

3. The Analytical Grid for the Exercise of the Mandate under Article 16 TFEU and for the Contributions to this Mandate

The research question led to an analysis of how the European Union and the actors within the Union can best ensure internet privacy and data protection, within the constitutional safeguards provided for under EU law, in a manner that is legitimate in a democracy, subject to the rule of law, and, at the same time, effective in view of the huge challenges in an information society.

The previous chapters described in detail how the European Union exercises its mandate under Article 16 TFEU and how the different institutional actors and roles contribute to the success of the mandate. These chapters demonstrated that the contributions of the different actors and roles raise a variety of issues. These issues are not similar for each and every actor and role, despite the fact that the aspirational goals are the same: contributing to the respect

\[2610\] These three notions do not necessarily overlap. See Chapter 6, Section 13 of this study.
of privacy and data protection. This explains the diversity in focus in the chapters of this study.

This section provides an analytical grid for the exercise of the mandate and the contributions to the exercise of this mandate of the different actors. This grid will be used for assessing the various contributions and is designed as follows.

<table>
<thead>
<tr>
<th></th>
<th>Article 16 TFEU</th>
<th>Constitutional safeguards under EU law</th>
<th>Legitimacy</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Union</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CJEU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU legislator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperation mechanisms of DPAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU as external actor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This analytical grid has four components. First, Article 16 TFEU, read in connection with Articles 7 and 8 Charter, defines the task of the European Union to ensure privacy and data protection. Second, constitutional safeguards under EU law impose limits on the exercise of the task. Third and fourth, conditions of legitimacy and effectiveness must be fulfilled to make Article 16 TFEU work. The difference between the first two components of the analytical grid (the provision of Article 16 TFEU and the constitutional safeguards) and the two last components (legitimacy and effectiveness) is that the first two are mainly legal requirements, whereas the last two are more policy considerations.

*The first component: Article 16 TFEU defines a broad mandate*

Article 16 TFEU provides a mandate for the European Union to act that is in principle unconditional. This mandate enables the Union – in principle – to act in accordance with its ambitions and take the leading role in ensuring the respect of data protection as a fundamental right, and by doing so regaining control over the processing of personal data in an internet environment.

Article 16 TFEU also gives the Union tools: Article 16 TFEU ensures the respect of privacy and data protection as fundamental rights for individuals, ultimately under control of the Court of Justice, it assigns to the EU legislator the task to lay down a legal framework for data protection, and, finally, it ensures control by independent data protection authorities. In an internet environment, the governance model of EU privacy and data protection also
implies a role for cooperation structures of independent data protection authorities, as well as for the European Union in general as an actor in the external domain.

The substance of the protection to be provided is laid down in Articles 7 and 8 Charter, as well as in the legislative instruments for data protection, particularly Directive 95/46. These instruments also describe the substantive limits of the competence of the European Union under Article 16 TFEU.2611

The second component: constitutional safeguards under EU law

This mandate of the European Union under Article 16 TFEU is not unlimited. The exercise of the mandate coincides with other mandates of the Union itself and with the Member States’ powers in related areas of government intervention.

Moreover, the exercise of the mandate is also delimited by the general safeguards of EU competence requiring the European Union to respect the national identities of the Member States, including national security,2612 and cultural differences. EU action must also comply with the principles of subsidiarity and proportionality and with the features of a system of executive federalism,2613 in which implementation, enforcement and the organisation of judicial protection are normally tasks of the Member States. This was all explained in Chapter 4.

Furthermore, the contributions of the actors and roles under Article 16 TFEU are embedded in the institutional positions of the various actors and roles under EU law, in respect of the institutional balance and the separation of powers.

The third component: legitimacy as a factor for success

In this study, legitimacy means in relation to the governance of privacy and data protection under EU law: ensuring that there is some degree of accountability towards political institutions.2614 In the specific context of external EU action, legitimacy has an additional element: the legitimacy of external EU action is also determined by – possibly conflicting – legitimate claims of third countries and international organisations.

Legitimacy in this domain is not self-evident, for various reasons. First, under Article 16 TFEU, the protection of a fundamental right is a task of the European Union, which is often criticised for its democratic deficit. Second, the mandate requires the involvement of actors outside the traditional trias politica who are not subject to full democratic control by parliaments, such as particularly the DPAs as expert bodies. Third, the link between the

---

2612 Article 4(2) TEU.
2614 As explained in Chapter 1, using the wording in the CJEU’s case law on the independence of the DPAs.

457
cooperation mechanisms of DPAs – operating in between the Union and the Member States – and political institutions is weak. Fourth, the involvement of the private sector in the exercise of the mandate under Article 16 TFEU further weakens democratic guarantees.

Against this background, the European Union should take into consideration that individuals have justified claims that the democratic accountability be ensured and that decisions be taken at a level “as close as possible to the citizen”. 2615

The European Union should also take justified claims of national governments into consideration. The mandate of the Union under Article 16 TFEU contains an exception to the main rule in the EU system that the protection of fundamental rights is a core task of national governments that should be fully democratically accountable. The exercise of the mandate under Article 16 TFEU could, to a certain extent, deprive Member States of the power to protect the fundamental rights of their nationals. 2616

Finally, the European Union has justified claims vis-à-vis third countries in respect of activities on the internet and is, vice versa, confronted with similar justified claims of third countries and international organisations. In theory, the Union acting as a guardian of privacy and data protection would be most effective if it could claim jurisdiction over the entire internet. However, this claim would coincide with legitimate claims of third countries and international organisations, because jurisdictions overlap on the internet. This is particularly problematic in cases where other jurisdictions have made different arrangements for privacy and data protection. 2617

**The fourth component: effectiveness as a factor for success**

High standards of effectiveness are required in view of the phenomena on the internet that challenge privacy and data protection. Effectiveness is a general principle of EU law that was specified in this study for the purposes of the governance of privacy and data protection: ensuring protection by bridging the gap between principles and practice. 2619 Involvement of various stakeholders, including the private sector, in the implementation is a component of the governance under Article 16 TFEU in order to deliver privacy and data protection in an effective manner.

Effective exercise of the mandate under Article 16 TFEU gives legitimacy to the EU action itself. Legitimacy based on effectiveness (output legitimacy) justifies the capacity of the European Union to act and to impose rules in a global environment, to involve private parties, and to attribute tasks to the independent data protection authorities, which are non-

---

2615 Article 1 TEU.
2616 Judge Masing of the German constitutional court claimed that this would result from the General Data Protection Regulation; see: “Ein Abschied von den Grundrechten”, Süddeutsche Zeitung 9 January 2012.
2617 As explained in Chapter 9.
2618 As explained in Chapter 1, with reference to Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, Chapter 8. As explained in Chapter 9.
majoritarian expert bodies. However, output legitimacy alone is not sufficient for EU action in privacy and data protection. Democratic legitimacy (or input legitimacy) is also required.

4. The Contribution of Article 16 TFEU to Legitimate and Effective Privacy and Data Protection on the Internet: An Appropriate Mandate is provided

This section describes how Article 16 TFEU contributes to legitimate and effective privacy and data protection on the internet. It outlines a general framework enabling the various actors and roles to make Article 16 TFEU work.

*Article 16 TFEU brings privacy and data protection by definition within the scope of EU law and makes ambitious approaches possible (the first component)*

As a result of Article 16 TFEU, privacy and data protection fall by definition within the scope of EU law. Privacy and data protection have become concerns of the European Union, although the implementation is shared with the Member States. The EU mandate in this field is also broad in terms of substance: privacy and data protection are considered to be one complex of concerns, particularly in an internet environment, based on human dignity, autonomy and fairness. The right to privacy – in a wide sense – represents the value, whilst the right to data protection determines the rules of the game.

Privacy and data protection are part of a European Union based on values. The European Union has high ambitions in promoting its values, particularly democracy, the rule of law and fundamental rights. These three values are inextricably linked. These values are shared between all the Member States and represent the premise of mutual trust amongst the Member States themselves and between the Member States and the Union.

The European Union has ambitions to promote democracy, which, in relation to the internet, means a free internet but not an unprotected internet. The Union has ambitions to promote the rule of law, which, in relation to the internet, “requires as a minimum that the law actually rules”, meaning that the law should also be respected on the internet. The Union has ambitions to promote fundamental rights, which, in relation to the internet, means that fundamental rights should be applied broadly, with a strong focus on protecting individuals in horizontal situations, against private parties.

Promoting fundamental rights in an internet context entails at least two things: first, individuals are entitled to the protection of fundamental rights when they are active on the internet (online), in the same way as when they act in any other capacity (offline); second, the external dimension – protection vis-à-vis actors in third countries – acquires a new dimension because individuals in the European Union interact on the internet on a constant basis with actors based outside the Union. However, individuals are not entitled to protection against all risks on the internet. A zero risk approach does not exist.

---

2620 Armin von Bogdandy, Michael Ioannidis, “Systemic deficiency in the rule of law: What it is, what has been done, what can be done”, CMLR 51 (2014), Issue 1, pp. 59-96, p. 63. See Chapter 2, section 5 of this study.
Article 16 TFEU makes it possible, with these notions in mind, for the European Union to realise its high ambitions by giving priority to ensuring privacy and data protection on the internet. By making Article 16 TFEU work, the Union should compensate for phenomena resulting from developments on the internet. Compensation is needed because, as was explained above, the internet as a networked society leads to insecurity and a lack of grip. Internet freedom is threatened by fragmentation of the internet, by asymmetry in relation to big data and by secrecy in relation to surveillance.

The constitutional safeguards under EU law: the Member States play and should play an important role (the second component)

First, the mandate under Article 16 TFEU does not mean that the European Union is the sole guardian of EU data protection. The Member States play and should play an important role. To start with, the exercise of the EU mandate should comply with the principles of subsidiarity and proportionality. The exercise of the mandate by the Union under Article 16 TFEU gives a priori effect to the principle of subsidiarity, since efficient and effective privacy and data protection on the internet cannot be sufficiently achieved by the Member States individually.

Second, the European Union should respect national identities, national security and cultural differences. The exemption of national security from the scope of EU law played a role in the aftermath of the Snowden revelations. This study explained that this exemption plays a limited role in the area of privacy and data protection. The exception to the scope of EU law for national security does not mean that a justified claim based on national security under Article 13 of Directive 95/46 on data protection renders EU law inapplicable. The ruling of the Court of Justice in ZZ2621 even provides an argument in support of the application of general EU data protection law to national security services. The exception to the scope of EU law does not extend to authorities of third countries, although they may be covered indirectly. In short, even in the domain of national security, the entitlement of the individual to privacy and data protection should be decisive, which means that the scope of the national security exception should be interpreted restrictively.

Third, as a rule, within the European Union as a construct with features of executive federalism, implementation of EU law is decentralised. Moreover, under EU law, the enforcement of EU instruments and the organisation of judicial protection are normally tasks of the Member States. However, the decentralisation of the implementation should not adversely affect the harmonised level of protection. To avoid this undesired result, cooperation is required between the different actors of the Union and the Member States, under the principle of sincere cooperation.

Legitimacy as a factor for success for EU action (the third component)

2621 Case C-300/11, ZZ, EU:C:2013:363.
This study claims that a legitimate and effective exercise of the mandate of the European Union on privacy and data protection, a field of intervention that affects the daily lives of individuals, makes the Union more visible and shows that it is capable of successfully addressing major challenges.

The success of EU action in this field is even more relevant in view of the presumed democratic deficit of the European Union. It is submitted that solutions – albeit imperfect – have been found for issues relating to the more formal aspects of democratic legitimacy, for instance by granting the European Parliament more powers. However, this does not resolve what Weiler calls the crisis of social legitimacy.\textsuperscript{2623} The European Union is not perceived as an organisation of the citizens. Although European leaders may speak in name of the people, many people are not aware that they are doing so.\textsuperscript{2624}

Hence, the European Union should take into consideration justified claims of individuals that democratic accountability is ensured and that decisions are taken at a level “as close as possible to the citizen”.

The concept of EU citizenship further contributes to the legitimacy of the role of the European Union under Article 16 TFEU. EU citizenship justifies the expectations of EU citizens that their rights will be protected. The exercise of the mandate under Article 16 TFEU contributes to the genuine enjoyment of citizenship of the Union. Vice versa, this contribution to the enjoyment of citizenship gives legitimacy to the exercise of the EU mandate under Article 16 TFEU.

EU action should not only be legitimate in the eyes of the citizen, but also vis-à-vis the Member States. Legitimacy of EU action under Article 16 TFEU, in the sense of creating guarantees for some degree of accountability vis-à-vis political institutions, is a prerequisite for trust, particularly in the domain of privacy and data protection. The protection of these rights is closely related to traditional state functions belonging to the core of a democracy, which is subject to the rule of law.

The European Union and the Member States interact in a pluralist legal context, with overlapping claims to legal and constitutional authority. Article 16 TFEU confers a broad and relatively unlimited power on the Union, to regulate the sensitive area of data protection. Article 16 TFEU has as an effect that to a certain extent Member States could be deprived of the power to protect the fundamental rights of their nationals, as explained above.

The legitimacy is even more at stake where the private sector plays a role in core government activities, such as the combat of terrorism and serious crime. These are sensitive areas,

\textsuperscript{2623} The Constitution of Europe, “Do the new clothes have an emperor?” and other essays on European integration, Joseph Weiler, Cambridge University Press, 1999, p. 84.

\textsuperscript{2624} Middelaar, Luuk van, 2009, De passage naar Europa. Geschiedenis van een begin (published in English as: The Passage to Europe: How a Continent Became a Union), Historische Uitgeverij, part III.
requiring additional safeguards such as appropriate oversight mechanisms. The European Union should ensure that these safeguards are respected.

Finally, the principle of sincere cooperation has gained in importance in view of the loss of power of the Member States, and also in view of the loss of control over personal data on the internet. Cooperation between the different levels and actors should compensate for the loss of power of – individual – public entities within a globalised society and hence enhance the legitimacy of ensuring privacy and data protection.

*Effectiveness as a factor for success for EU action (the fourth component)*

The presumed lack of effectiveness of privacy and data protection triggered this study and is also a key justification for the reform of the data protection legislation in the European Union.\(^{2625}\) Citizens may expect the Union to be able to exercise its mandates in an effective manner. This gives the Union legitimacy (output legitimacy). As the Snowden revelations illustrate, output legitimacy is not self-evident and control over privacy and data protection on the internet should be regained. Control requires high standards of effectiveness in view of the phenomena on the internet that challenge privacy and data protection.

This study applied the general principle of effectiveness under EU law to the governance of privacy and data protection: ensuring protection by bridging the gap between principles of privacy and data protection and practice. Bridging the gap requires an appropriate choice of arrangements,\(^{2626}\) strengthening the various actors and roles under EU law. EU legislation should facilitate the contributions of the judiciary, the independent data protection authorities, the cooperation mechanisms of these authorities, as well as the European Union as an external actor.

In this study, emphasis was placed on instruments encouraging the involvement of various stakeholders, including the private sector, in the implementation of the governance under Article 16 TFEU. The involvement of various stakeholders does not affect the final responsibility for ensuring privacy and data protection. This final responsibility remains with governmental actors and, ultimately, the European Union. Effective governance requires firstly empowerment of the individual, secondly giving responsibility to the data controllers with multi-stakeholder solutions as an alternative for command-and-control legislation, and thirdly strong enforcement mechanisms.

*Final recommendation*

Article 16 TFEU provides the European Union with a strong mandate and ensures that privacy and data protection, by definition, fall within the scope of EU law. The high ambitions of the European Union resulting from this mandate should compensate for the

\(^{2625}\) As explained in Section 10 below.

\(^{2626}\) The word ‘arrangement’ is used to distinguish from the legislative ‘instruments’, in the EU context mainly regulations and directives.
presumed lack of control on the internet. The Union is not the sole guardian of privacy and data protection on the internet. The Member States also have a role. The executive federalism should not adversely affect the harmonised level of protection.

An appropriate exercise of the mandate under Article 16 TFEU contributes to the Union’s social legitimacy and can also be an element of the enjoyment of EU citizenship. EU action should also be legitimate vis-à-vis the Member States. Effective exercise of the mandate provides the European Union with output legitimacy. Bridging the gap between principles of privacy and data protection and practice requires an appropriate choice of legislative arrangements, strengthening the various (public) actors and roles under EU law, as well as involving the private sector and leaving the final responsibility with governmental actors.

This study includes a number of ideas on the involvement of the various public and private actors in the governance of internet privacy and data protection. The study recommends elaborating these ideas and developing a strategy for this involvement that clearly describes the responsibilities of the various actors.

5. The CJEU interprets the Law in Cases brought before it and acts as Constitutional Court

Article 16(1) TFEU and the guidance in final instance by the CJEU (the first component)

The Court of Justice of the European Union does not only interpret the law by solving the disputes brought before it or by answering preliminary questions of national courts, resulting from disputes arising in the national jurisdictions. In the exercise of its tasks, the Court also acts as a constitutional court, with three functions: the reviewer of fundamental rights, the protector of market integration and the umpire between the different powers. This role as a constitutional court, combined with a – perceived – activist approach in the exercise of this role qualifies the Court as a suitable actor for privacy and data protection on the internet.

Obviously, in this field, the main contributions of the Court of Justice acting as a constitutional court serve the first function, the review of fundamental rights. It is the task of the Court to ensure, in last instance, that everyone’s rights to privacy and data protection are respected. The case law demonstrates that the Court contributes in different ways to ensuring the enjoyment of these rights. The Court interprets the rights to privacy and data protection under EU law, balances these rights with other fundamental rights and public interests, contributes to the governance model by setting the standards for the independence of data


\[2628\] See Chapter 5, Section 3 of this study, with reference to Paul Craig and Grainne de Búrca, EU Law, Text, Cases and Material, Fifth Edition, Oxford University Press 2011, at 63-65.

\[2629\] A recent example is Case C-212/13, Ryneš, EU:C:2014:2428, on the interpretation of the household exception.

\[2630\] A recent example is Case C-580/13, Coty Germany, ECLI:EU:C:2015:485, on balancing with the fundamental right to an effective remedy and the fundamental right to intellectual property.
protection authorities, and deals with extraterritorial jurisdictional claims of EU law, in particular by basing the claim of EU jurisdiction on a meaningful link with the European Union in ensuring the protection of the individual.

The Court deals with the remarkable elements of Article 16 TFEU and Article 8 Charter. As an example, the interpretation of the right to data protection under Article 8(2) Charter draws on the acquis laid down in Directive 95/46 on data protection. This reasoning is circular, since the Court interprets Directive 95/46 in the light of the Articles 7 and 8 Charter.

Often, the contribution of the Court of Justice consists of giving guidance, where it adjudicates in cases by explaining EU data protection legislation in the light of the Articles 7 and 8 Charter. Cases end up at the Court on the basis of preliminary questions referred by national courts on the explanation of Directive 95/46 or of other legislative instruments relating to privacy and data protection.

For the Court, an important perspective is and will increasingly be that the reality of the internet is difficult to reconcile with core data protection principles. ‘Consent’ and ‘purpose limitation’ are examples of such principles that the Court may have to interpret, whilst taking into consideration the developments in the information society. These developments also influence the balancing with other interests since fundamental rights and public interests increasingly coincide.

More generally, the assessment by the Court of Justice of limitations applicable to a fundamental right focuses on proportionality. The entry into force of the Lisbon Treaty prompted a fundamental change of the approach of the Court in relation to fundamental rights. In this approach, the Charter has become the yardstick and has a wide scope, without extending the competences and tasks of the European Union. The proportionality test under the Charter is strict; the strictness in a concrete situation depends on a number of factors. The nature of the fundamental right is such a factor. This factor is elaborated in this study, which analyses whether meaningful distinctions can be made between the fundamental rights that must be protected on the internet.

The constitutional safeguards under EU law: a judiciary explaining the boundaries with other mandates in an information society (the second component)

This study distinguished two different types of safeguards flowing from the role of the Court of Justice within the EU constitutional framework, in relation to Article 16(1) TFEU.

The first type of safeguards is institutional, relating to the role of the judiciary. Most cases are brought before the Court in the context of the preliminary ruling procedure. This procedure is

---


2633 The example is Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
a success, also in privacy and data protection. The preliminary ruling procedure enables the Court to provide guidance, also in important issues. However, the case law of the Court is by definition incremental. It is not the role of a court to develop a policy for better protection. Therefore, guidance by the Court is not sufficient for bridging the gap between general principles and practice. Bridging the gap requires contributions of actors that can develop a comprehensive policy, such as the EU legislator and the independent DPAs.

The second type of safeguards is substantive: the exercise of the mandate of the European Union under Article 16 TFEU is limited by mandates of the Union in other fields and by the competences of the Member States. Ensuring privacy and data protection requires balancing privacy and data protection with other fundamental rights and essential interests, in the specific internet context. This balancing plays a key role in the case law of the Court, as the following examples illustrate.

First, the link between the fundamental rights of privacy and data protection, on the one hand, and the freedom of expression and information, on the other hand, is changing and intensifying due to internet-related developments. The dividing line between private and public speech is becoming blurred on the internet. Changes are caused by the impact of a free and open internet on privacy and data protection, whereas new intermediaries, like search engines, play a role in promoting the freedom of expression and information.

The debate on the right to be forgotten demonstrates that where an individual is entitled to request the deletion of personal data, this automatically has an impact on the right to receive information under Article 11 Charter. In Google Spain and Google Inc., the Court accepted this consequence, taking the changed reality in the information society into consideration. This changed reality has an impact on privacy and data protection and on the balancing of fundamental rights. The ubiquitous availability of information implies a lack of control of the data subject and affects his autonomy. This ruling of the Court is not undisputed. For instance, the case law of the US Supreme Court shows a different approach in balancing privacy and with free speech, with more emphasis on free speech. At the same time, Google Spain and Google Inc. was heavily criticised in the US and by various European scholars, because of its presumed impact on free speech and democracy. Although this study does not support this criticism, admittedly, the ruling does not precisely define the boundaries between the fundamental rights at stake. Further case law may be needed.

In Google Spain and Google Inc., the Court also took the changed reality in the information society into consideration in another respect. The Court gave search engines a social responsibility, attributing to them the task of the balancing of fundamental rights, after they have received requests for the deletion of links containing personal data.

---

2635 E.g., in Sorrell v. IMS Health Inc., No. 10-779 131 S.Ct. 2653 (2011), see Chapter 5, Section 11.
2637 E.g., in Case C-398/15, Manni (pending).
Second, the right of access to documents gives effect to core values in society as transparency, which includes the right to know, and democratic control. The Court scrutinises the exceptions and limitations to this right restrictively. However, the same restrictive approach is not applied where the Court balances the right of access to documents with privacy and data protection. Under the Court’s case law, applicants who request access to documents of the European Union must demonstrate the necessity for having access to documents if these documents include personal data. The Court does not seem to balance privacy and data protection on an equal footing with public access to documents, but seems to give more weight to privacy and data protection.

Third, there are different scholarly views on the status of the right to property as an essential value in a democratic society. The right to property is not included in all fundamental rights treaties although it plays an important role in the application of the ECHR. This study argues that privacy and data protection, on the one hand, and property and especially intellectual property, on the other hand, should not necessarily be balanced on equal footing. The example in support of this argument is the enforcement, on the internet, of copyright, which is an intellectual property right. Since copyright is difficult to enforce on the internet, copyright holders claim that the monitoring of the behaviour of all individuals on the internet is needed to enforce their copyrights. Recognition of this claim would obviously weaken the level of privacy and data protection. In view of the essential nature of privacy and data protection in our democratic societies, it is submitted that, where both rights need to be balanced against each other, the rights to privacy and data protection should carry greater weight than the right of the rights holder.

Fourth, the relationship between privacy and data protection and security has elements of a trade-off. Privacy is, on the one hand, seen as inhibiting the appropriate protection of our societies against threats caused by terrorist attacks or by serious crime and, on the other hand, as a value that should prevail against risks of unconditioned surveillance. Digital Rights Ireland and Seitlinger gives indications for balancing privacy and security, with an emphasis on the intrusiveness of monitoring of individuals in an information society. The study includes an interesting parallel with the approach of the US Supreme Court. The US Supreme Court, too, considers the intrusive consequences of the information society. For instance, the US Supreme Court decided that generally a warrant is needed before the search of a smartphone, because of the immense storage capacity of a device people carry on them. A smartphone is not just a physical device that people have on them, but can provide – when it is searched – a broad insight into the private life of individuals.

More generally, the outcome of the trade-off between privacy and data protection and security is determined by trends in these two areas: the effects of ubiquitous connectivity for

---

2639 As explained in Chapter 5, Section 15 of this study.
2640 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.
2641 Riley v California, No. 13–132.
privacy and data protection, on the one hand, and the security threats for society, on the other hand. Moreover, it proved difficult to measure these trends and to measure the effects of proposed instruments and to make comparisons on the basis of this measurement.

Other arguments that should play a role in the trade-off are: (a) the lack of transparency of government surveillance should be addressed, (b) the value given to privacy and data protection should not depend on political preferences of a majoritarian body, and (c) strong privacy and data protection can benefit law enforcement. The challenge is to find synergies.

Legitimacy as a factor for success of the CJEU (the third component)

In a general sense, the extensive role of the Court of Justice compensates for the democratic deficit of the Union. The Court has further legitimacy because of its close connection with national courts through the preliminary ruling procedure. The Court enhances its legitimacy by properly balancing the interest of EU integration with national interests.

The challenges for internet privacy and data protection justify an emphasis on context-related balancing with other fundamental rights taking into account that the internet does not pose the same challenges for all fundamental rights. Freedom of expression is an example:2642 as a rule, the internet is a vehicle for the freedom of expression, not a challenge. This balancing is at the heart of the contribution of the Court to the exercise of the mandate under Article 16 TFEU, more than it is for the other actors and roles under Article 16 TFEU. Where the Court succeeds in striking an acceptable balance between the various interests concerned, this increases the legitimacy of EU action under Article 16 TFEU.

This study claims that the legitimacy of the European Union, in general, and the Court, in particular, can even improve if distinctions are made between fundamental rights (and essential interests), in the sense that not all rights and values are balanced on an equal footing, albeit without establishing a hierarchy between rights.

Making a distinction between fundamental rights can be useful for three purposes. First, this should prevent any weakening of privacy and data protection (and other fundamental rights that are most crucial for our democracies), which could result from the equal protection of all rights, by allowing a differentiation in the standard of review for the different fundamental rights enabling a high standard of protection for these most crucial fundamental rights. Second, the distinctions should assist in compensating for the particular challenges of certain rights on the internet, and enable an efficient use of resources. Third, these distinctions would make it possible to focus on extraterritorial application of fundamental rights, taking into consideration legitimate claims of third countries or international organisations.

Extraterritorial application of EU law in certain fields of EU intervention such as privacy and data protection is legitimate, precisely because the core values of Article 2 TEU – particularly

2642 As illustrated by the CJEU in Case C-131/12, Google Spain and Google Inc., EU:C:2014:317.
democracy, the rule of law and fundamental rights – are at stake. This legitimacy does not necessarily exist to the same extent for all fundamental rights included in the Charter.

The Charter does not establish a hierarchy between fundamental rights. This study proposes a simple taxonomy that would permit to apply different standards of review in respect of fundamental rights protection on the internet, without creating a hierarchy. This taxonomy would serve the three purposes mentioned above, and would enable an efficient use of resources, whilst also taking a focused approach on extraterritorial application. The study suggests that the legitimacy of the role of the Court would further improve, if the Court were to assess, in a systematic manner, the application of the rights to privacy and data protection, taking into account this simple taxonomy. Privacy and data protection fall within the category of fundamental rights that have a high impact on human dignity.

This means more concretely that: (1) there is a necessity of protection in an online environment; (2) where needed, extraterritorial application of the rights must be safeguarded; (3) the rights should be applicable in horizontal relations; (4) restrictions and limitations of these rights are subject to a strict test; (5) where a balance is needed with other fundamental rights and public interests, the essential nature of the rights to privacy and data protection should be taken into account; and (6) this may lead to an approach where the Court adjudicates itself, and does not defer the matter to the national courts (in preliminary ruling procedures). These requirements are in line with the current practice of the Court on privacy and data protection.

Effectiveness as a factor for success of the CJEU (the fourth component)

Effectiveness is a key factor in the case law of the Court of Justice. Effectiveness is an important perspective in the Court’s interpretation of everyone’s rights to privacy and data protection. Effectiveness is a guiding principle for the Court, also where it assumes the role of promoting integration (on markets and elsewhere) and where it acts as an umpire in situations where other public interests or other governmental actors have an impact on the exercise of Article 16(1) TFEU.

Integration (on markets and elsewhere) is an additional interest to be taken into account by the Court, where it rules on the basis of Article 16 TFEU. The integration of data protection law in the European Union is to a large extent based on considerations of effectiveness, based on the view that fragmentation would weaken the protection. Forum shopping by big internet companies, in the sense of choosing a forum in a Member States with a perceived low level of protection in a fragmented Europe, is the example of a practice that may weaken the protection.

The Court acts as an umpire between different powers. Precise answers by the Court are required, in compliance of the principle of effectiveness, where the Court adjudicates on the boundaries between competences under Article 16 TFEU and relating competences.
Final recommendation

In recent years, the Court Of Justice played an important role in promoting privacy and data protection, also taking into account the impact of the information society. Two rulings in 2014, Google Spain and Google Inc, and Digital Rights Ireland and Seitlinger, are the best illustrations of a court taking privacy and data protection seriously.

This study makes the recommendation to base the scrutiny of fundamental rights on a simple taxonomy. This taxonomy of fundamental rights is structured as follows:

a. Non-derogable or absolute fundamental rights, corresponding to the rights included in Title I of the Charter, entitled dignity;

b. Rights with a huge impact on the human dignity, but not qualified as non-derogable;

c. Social, cultural and economic rights.

Further categories include: principles in the Charter (as meant in Articles 51(1) and 52(5) thereof), the fundamental freedoms of the Treaties relating to free movement, the undefined species of public and general interests.

6. The European Parliament and the Council lay down the Rules, whilst Respecting the Role of the Member States under Article 16(2) TFEU

Article 16(2) TFEU and the exhaustive nature of the EU legislator’s task (the first component)

The mandate of the European Union to act under Article 16 TFEU is widely formulated, and gives the Union the opportunity to realise its ambitions. Article 16(2) TFEU must be seen as an explicit choice of the authors of the Treaty to bring data protection to the Union level, by giving the European Parliament and the Council, in their common capacity as the EU legislator, the duty to lay down the rules. The European Parliament and the Council must act in accordance with the ordinary legislative procedure, on the basis of a proposal by the European Commission.

Article 16(2) TFEU contains a duty to adopt EU legislation: the EU legislator shall adopt the rules on data processing. The material scope of the rules includes all personal data. An exception to the material scope, excluding certain types of personal data – such as pseudonymised data – from the EU rules, cannot be laid down in secondary EU law. The European Union shares the competence under Article 16(2) TFEU with the Member States. However, there is not much autonomous room for the Member States to adopt legislation in this area. The entry into force of the General Data Protection Regulation, in particular, will take away most of the remaining Member States’ autonomy.
The data protection reform – with the General Data Protection Regulation as the centrepiece – should lead to the full implementation of this duty of the EU legislator, also in domains where at present EU rules are lacking.²⁶⁴³

The mandate under Article 16(2) TFEU runs a parallel with the competence of the EU legislator under Articles 18 and 19 TFEU on equal treatment and non-discrimination. Both mandates deal with fundamental rights, although they both have their origins in the internal market. High standards of effective protection are observed in both areas, due to this enhanced status. However, under Articles 18 and 19 TFEU, the Member States may still claim discretionary powers and require a higher level of protection under national law. These discretionary powers do not exist under Article 16(2) TFEU, for instance because of the importance of a uniform level of data protection in the digital single market.

The constitutional safeguards under EU law: a regulation as the appropriate instrument and a legislator confronted with interfaces with other competences (the second component)

The expected adoption of the General Data Protection Regulation – an EU regulation replacing an EU directive – as the main instrument for data protection is an appropriate choice of legislative instrument. This regulation should not only ensure a high level of protection, but also a harmonised level. In the context of the negotiations on the General Data Protection Regulation, it was discussed whether – in the light of subsidiarity – protection in the public sector should not be left to the Member States, or whether it should be subject to a specific regime with limited harmonisation making it possible that Member States complement the EU rules.²⁶⁴⁴ This study took the position that a specific approach in the public sector would not be an appropriate choice of instrument: there should be no distinction in law between the private and the public sector. The individual deserves equal protection in the public and the private sector. The fact that the Member States play and should play an important role should not result in an unsatisfactory choice of instruments.

Moreover, in the exercise of its mandate, the EU legislator is confronted with interfaces with competences of the European Union itself and of the Member States in related areas. These interfaces have an impact on the mandate under Article 16 TFEU. This study identifies specific areas where interfaces exist: the freedom of expression and information where the Union has limited competence, but where internet developments have a big impact on the enjoyment of the freedom; open data and the interface between transparency and data protection; and measures for internet monitoring with the aim of enforcing intellectual property rights.

Furthermore, EU data protection affects core competences of Member States and therefore the Member States have a legitimate role to play, although often by delegation. The study

²⁶⁴³ Such as the processing of personal data in the police and judicial sectors in the absence of cross-border elements, Article 1(2) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.
mentions five categories of provisions where the Member States should exercise competence in privacy and data protection.\textsuperscript{2645} First, EU law builds on national law where national law provides a ground for the processing of personal data, for example in the public interest; second, EU law mandates national law to give effect to its provisions, for example where it obliges the Member States to establish data protection authorities; third, EU law allows or requires national law to specify EU rules; fourth, EU law allows or requires national law to depart from EU rules; fifth, provisions enabling the Member States to balance privacy and data protection with other fundamental rights, within their field of competence.

\textit{Legitimacy as a factor for success of the EU legislator (the third component)}

There is one EU legislator. However this legislator is composed of different institutions. The input of the three institutions involved in the ordinary legislative procedure, respecting the institutional balance, gives democratic legitimacy to the mandate of the EU legislator, with the nuances explained in Chapter 4 of this study. The input in the negotiations on the data protection reform explains this. As a rule, the European Parliament acts as a supporter of strong privacy and data protection, whilst the Council represents national concerns and the Commission is committed to integration.

In addition, involvement of Member States and national authorities is required, for reasons of legitimacy. The European Union acts internally within a pluralist legal context, with an important role for the Member States in accordance with the principle of subsidiarity. Three considerations are: first, minimise the impact of the uniform EU framework for data protection on competences of Member States (including core state functions); second, allow additional national standards to the extent they do not affect the \textit{effet utile} of the uniform EU framework; third, provide for implementation and control on national level with respect of the executive federalism of the European Union.

The EU legislator should also involve the private sector and civil society in the legislative process. Consultation of the different stakeholders in the decision-making process enhances the legitimacy of the process, provided the consultation takes place in a balanced and transparent way. This could lead to a better result that takes the different interests at stake into consideration.

The EU legislator should address the interfaces between privacy and data protection and security in an intelligent manner, also for reasons of legitimacy, taking into account the case law of the Court of Justice. Security is a priority for the European Union and the Member States, and national and EU laws are adopted allowing a wide use of personal data for security purposes. The EU competences in the area of freedom, security and justice focus on the coordination and cooperation between the Member States, for reasons of security. The use of these competences – for instance through EU legislation – facilitates the exchange of large

\textsuperscript{2645} Largely based on: European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at II.2.a.
amounts of personal data between police and judicial authorities on the national and the EU level, but should not unduly impact on everyone’s right to privacy and data protection.

There are important synergies between privacy and data protection, on the one hand, and economic interests, on the other hand. Addressing these synergies is primarily a task of the EU legislator and not of the Court of Justice, which adjudicates only when disputes are brought before it. The Court does evidently not play a role where the issue is to find synergies between different areas of intervention. Using synergies in different areas of intervention by the European Union and the Member States enhances the legitimacy of the contribution of the EU legislator under Article 16 TFEU.

Respect of privacy and data protection is supposed to create trust. Trust positively influences – or even boosts – growth and innovation. This consequence is, for instance, recognised, in connection with the Digital Agenda for Europe.2646 The concept of Privacy by Design2647 is the example. Using this concept must enhance trust in data protection and create economic incentives. The legal framework for electronic communications may create synergies,2648 because it gives governments responsibility in network governance, in contrast with the governance of the internet infrastructure, where governments have less of a role to play. Government responsibility in network governance could be used for enhancing control over the processing of personal data, provided governments take considerations of privacy and data protection into account in the exercise of this responsibility.

An example of synergy between privacy and data protection, on the one hand, and consumer protection, on the other hand, is Directive 2005/29 on unfair commercial practices,2649 which prohibits misleading omissions and requires transparency in business-to-consumer transactions. This directive could also be used as an instrument requiring internet services to apply transparent privacy policies.

Competition law has relevance in the context of this study, because the information economy is characterised by an asymmetric structure. In this information economy, personal data have become an asset. Companies acquire market dominance, precisely because they accumulate

2646 See: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final.
2647 Included – under the heading of “data protection by design or by default” – as an obligation to implement the appropriate technological and organisational measures in Article 23 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.
large amounts of personal data. At present, competition law and privacy and data protection are areas of EU intervention with little interconnection. However, an approach based on synergies would enhance the legitimacy of the European Union, demonstrating that different parts of bureaucracy are managing to join efforts in addressing challenges of the information society. This study suggests that these synergies should be addressed by the EU legislator, in further changes of the EU legislative framework.

**Effectiveness as a factor for success of the EU legislator (the fourth component)**

The outcome of a legislative process, which involves three institutions and various other actors, by definition has the features of a compromise. Compromise solutions are not necessarily the best solutions for dealing with privacy and data protection on the internet.

This prospect of a compromise makes an appropriate choice of legislative arrangements even more crucial. The starting point for the EU legislator is the choice of the legislative instruments as such. The Commission considers that a regulation is the best legal instrument for data protection, based on reasons that are – more or less – related to effectiveness. A regulation “will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.”

This study subscribed to this view of the Commission and focused on the substantive content of the legislative instruments, underlining that the arrangements within these legal instruments should give the right incentives to data controllers to effectively ensure protection on the internet. The Commission recognises the need for specific arrangements that anticipate the developments on the internet, more generally, in its Better Regulation Guidelines of 2015 and in policies under the umbrella of Smart Regulation. Multi-stakeholder solutions or multi-level governance is a concept that plays an increasing role in the governance of privacy and data protection in the European Union.

The involvement of the private sector and NGOs in the governance of privacy and data protection is necessary in view of their key role on the internet. Involvement of these stakeholders should take place recognising the responsibilities of new roles. Search engines having a quasi-public role in the distribution of information, as a result of Google Spain and Google Inc., are an example.

Furthermore, in accordance with the principle of effectiveness, the rules on privacy and data protection should be appropriate to face the challenges in the information society. This means, for instance, that they must provide an adequate response in a technologically

---

2650 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final, Explanatory Memorandum, at 3.1.


turbulent environment, by defining rules that are technology-independent and hence not too precise. At the same time, the mandate of the EU legislator should be exercised, taking into consideration that fundamental rights of individuals are at stake. This latter consideration imposes limits on the use of ‘open norms’ not giving sufficient legal certainty to the data subject.

Accountability of data controllers and data processors should play an important role as a legislative technique, allocating responsibility to those actors. Accountability is a concept, connected to corporate social responsibility. Accountability is an alternative for command-and-control legislation, based on general notions of quality of legislation. Accountability schemes such as company privacy programmes should be sufficiently precise. The relation of these schemes to the provisions of EU data protection law should be fully transparent.

Appropriate enforcement is needed as a key element of effectiveness. Under the rule of law judicial and other remedies must be easily accessible and complete, and the mechanism of protection must be transparent for the individual. The arrangements in the rules adopted under Article 16(2) TFEU for the DPAs and their cooperation mechanisms should ensure this.

Final recommendation

The study mentioned five directions for the European Union and the Member States to regain control of data protection on the internet. First, the existing legal instruments for privacy and data protection should be interpreted in a way that takes the changed circumstances into consideration; second, the legislative arrangements should be adapted to the new circumstances; third, the changed relationship between the public and the private sector should be addressed, by recognising a closer involvement of the private sector in the implementation of the law without questioning the final responsibility of government; fourth, the European Union and the Member States should focus their interventions on the essential components of privacy and data protection, for pragmatic reasons and for jurisdictional reasons; fifth, the European Union and the Member States could reconsider the main principles of data protection, in order to adapt these principles to the changed circumstances, however without losing sight of the need for protection of individuals. This fifth direction is for the long term, if only because the main principles of data protection are laid down in primary EU law.

These directions are relevant for the entire mandate of the European Union under Article 16 TFEU. However, the contribution of the EU legislator plays a key role in regaining control. A regulation is the appropriate legislative instrument, also for the public sector.

Data protection as a right to fair processing requires the legislator to give effect to the core elements of data protection, mentioned in the Charter. The focus in the General Data Protection Regulation is the adaptation of legislative arrangements to the new circumstances. One thing the regulation explicitly omits, is addressing the principles or values of privacy and data protection as such.
This study recommends developing a strategy for the legislator on how to regain control, based on the five directions mentioned above and focusing on the impact of the internet on the main principles of data protection. In the long term, this strategy could result in the rethinking of the principles or values of privacy and data protection.

7. Independent DPAs exercise Control as Expert Bodies with Full Independence, but are Not Exempted from Democratic Accountability

Article 16(2) TFEU and the variety of roles of the DPAs (the first component)

An essential part of the enforcement of EU data protection law is assigned to expert bodies, which are primarily the DPAs of the Member States. These DPAs are independent public authorities with a variety of roles: ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers. In short, not only is the Union’s mandate under Article 16 TFEU broad, but so is the mandate of the DPAs within the European Union and the Member States.

The embedding of the role of DPAs in primary law gives them constitutional status under EU law. In the information society, their role is justified by the size of the issues at stake, and by the fact that traditional methods of governance by the executive, legislative and judicial branches are not considered sufficient. These independent authorities fulfil an important public task, but they are not accountable for their performance to the democratically elected bodies.

The embedding of the role of DPAs in primary law also ensures that they have full competence under EU law, with a variety of roles attributed to them. Other European or national authorities – like national ombudsmen or agencies in neighbouring areas – can be competent to deal with data protection issues, but their competence does not derogate from the competence of the DPA. To give an example: an individual may have a right to submit a complaint relating to a data processing operation to an ombudsman or an agency in a neighbouring area. However, the exercise of this right to complain does not deprive the individual of his right to involve the DPA, nor does it affect the competence of the DPA to act of own motion.

The study identified six reasons behind the existence of DPAs. First, historical reasons; second, the need for structural support in the area of data protection; third, the nature of data processing and the skills for understanding data processing; fourth, the need for control of the private sector and, equally, of governments in their capacities of controllers or processors of personal data; fifth, the need for independence from political preferences; sixth, the capability to combine expertise and flexibility, and to dedicate their resources fully to data protection.

The constitutional safeguards under EU law: DPAs as non-majoritarian expert bodies (the second component)

First, from the institutional perspective, the DPAs are a new branch of government: they are non-majoritarian expert bodies. They are in some respects different from and in others similar to both national agencies recognised under EU law and EU agencies. Agencies enjoy autonomy. There are two main differences between agencies and DPAs. First, the agencies must respect general government policies, whereas the DPAs do not have to respect this type of guidance. Second, the requirements on what constitutes institutional independence are considerably less strict for agencies than for DPAs. There are two main similarities: First, DPAs as well as agencies are bodies composed of experts exercising public tasks and they function, in substance, quite similarly. Second, both DPAs and agencies operate in between the EU and the national levels.

This study qualified the DPAs as a new branch of government, according to the theory of Vibert.2654 DPAs do not derive their power from the other branches of government. They are not agents vis-à-vis a principal. By contrast, they are competent to supervise these other branches of government, the traditional trias politica. This new branch of government could be instrumental in restoring trust in public authority, if the authorities are completely independent and operate within a context of checks and balances. The DPAs should act within the limits of their competence in accordance with requirements of independence, effectiveness and accountability. Similar requirements have been developed for good governance of agencies.

Although EU agencies and DPAs are essentially different, they both are expert bodies in between the EU and national levels. EU agencies are EU bodies established under EU law, but, in return, the Member States have ensured that national influence is retained. DPAs are national bodies established under national law, but once established, they exercise tasks attributed to them by primary EU law. There is a tendency to allow national interests to play a greater role in the functioning of EU agencies. On the contrary, the national autonomy in relation to DPAs has diminished, and this will be even clearer under the General Data Protection Regulation.

Second, the DPAs should, in the exercise of their tasks, take into account that they are public authorities and that ensuring control is their main task. DPAs should not consider privacy and data protection in isolation, but should take into consideration that in a democratic society subject to the rule of law other fundamental rights and essential interests also deserve protection. The DPAs exercise a variety of (advisory) tasks, but should ensure that this does not affect their core role, ensuring control.

Legitimacy as a factor for success for the DPAs (the third component)

The legitimacy of the DPAs is, on the one hand, based on their independence. On the other hand, the legitimacy of DPAs is related to the fact that, under the Court of Justice’s case law, this independence does not fully exempt them from accountability towards parliaments, although this does not apply to their performance in specific cases. Parliamentary influence is by definition limited.

The legitimacy of DPAs also derives from their accountability to the judiciary under the rule of law. As the General Data Protection Regulation confirms, everyone has the right to a judicial remedy against decisions of a DPA concerning him or her. In addition, the judicial accountability is a compensation for the loss of full parliamentary control.

The DPAs are completely independent, as has been confirmed by the Court of Justice. Under the Court’s case law, reliability of supervision is an objective, because supervision affects the social sphere of individuals. Independent, reliable supervision contributes to legitimacy. Independence is supposed to make the supervision more reliable. This is one argument for explaining the high standards of independence. Under the Court’s case law no external influence is allowed. The high standard for independence also means that there should be sufficient organisational distance to the executive. The task of the DPAs includes the balancing of various interests, which, according to the Court, requires distance from majoritarian policy-making, to ensure a fair decision-making process.

The complete independence of the DPAs confirms their status as a new branch of government and differs from the autonomy of EU agencies, which is understood as meaning autonomy from the influence of market forces, but not from political majorities. The DPAs themselves, too, have an obligation to safeguard their own independence vis-à-vis the other branches of government and the private sector.

The DPAs should, in the exercise of their tasks, act in an independent manner, but with full respect for their position in constitutional frameworks. The variety of tasks of DPAs may conflict with each other. For example, a DPA may, as a policy advisor, oppose a proposed legal instrument. However, after adoption of the instrument, the DPA should enforce the instrument. Another conflict of tasks may arise where DPAs cooperate with private entities, in developing frameworks for compliance, whereas they may be called upon to independently assess these frameworks at a later stage in the context of a complaint procedure.

The appointment of members of DPAs is a critical factor for the independence of DPAs. This study suggested involving the legislative, the executive and the judiciary branches in the appointment procedure, to ensure checks and balances and to avoid political preferences from playing a decisive role in the appointment.

The national DPAs are, on the one hand, part of the national administration and, on the other hand, they act as agents of the European Union. This positioning is in accordance with the

principle of subsidiarity, but it further complicates their democratic legitimacy, and also the judicial accountability. It is not clear whether the DPAs are – primarily– accountable at the national level or at the EU level.

From the perspective of legitimacy, expert bodies should not act in a non-controllable and arbitrary manner. The study distinguished three perspectives based on the work of Bovens.\textsuperscript{2656} Under the democratic perspective, the DPAs should ensure transparency of their performance to the public. Under the constitutional perspective, checks and balances for DPAs should be found in judicial control, the application of financial rules and control by a court of auditors. From the learning perspective, DPAs should profit from peer reviews, impact assessments and engaging with external experts.

Finally, considerations of legitimacy also have an impact on the prior involvement of DPAs in accountability schemes, set up by data controllers as a practical approach to promote bridging the gap between principles and practice. This involvement may increase the quality of the schemes from the perspectives of privacy and data protection, but should, generally, not bind these authorities in the exercise of their enforcement role, particularly where they are acting in response to individual complaints. Co-responsibility of data protection authorities – for instance through endorsement of accountability schemes – should be avoided, because it may adversely affect the independence of the DPAs.

\textit{Effectiveness as a factor for success for the DPAs (the fourth component)}

DPAs should have effective powers, particularly in the developing information society. Member States should guarantee protection by DPAs, in accordance with the general EU principles of equivalence and effectiveness.

The effectiveness of DPAs is a subject of debate, for instance where the enforcement in the EU is compared with the enforcement in the US where there are no DPAs. The most visible enforcement body in the US is the Federal Trade Commission (FTC). FTC enforcement is described by several scholars as a big success factor of the protection in the US, delivering ‘privacy on the ground’. They emphasise the large amount of financial penalties imposed, as well as the forward-looking injunctions. By contrast, in the EU, there is a presumed lack of effectiveness and the DPAs struggle for resources.\textsuperscript{2657}

Also, the Fundamental Rights Agency of the European Union reported that there is a great variety of, as well as significant deficiencies in, the powers and resources of DPAs. The Agency reported on understaffing and lack of adequate financial resources of DPAs, with the result that in many Member States the DPAs do not carry out all their tasks. As a rule,


\textsuperscript{2657} Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions, Amsterdam / Cambridge, September 2015, at II A.
sanction powers are limited and not suited to effectively address infringements by big internet companies, although the sanctioning powers are gradually changing.\textsuperscript{2658}

In addition, current EU law permits forum shopping by big internet companies, which implies that these companies can choose to set up their main establishment in a Member State with a perceived low level of DPA enforcement. Vice versa, a DPA is not permitted to enforce data protection law, if an internet company chooses an establishment abroad, whilst targeting individuals within the Member State where the DPA functions.\textsuperscript{2659}

The effectiveness of DPAs is a major issue in the reform of the EU data protection framework. The General Data Protection Regulation does not embrace the alternative of the US model, but aims at addressing a number of shortcomings, ensuring strong powers – including sanctioning powers – of the DPAs. Until the entry into force of the proposed regulation, it continues to be an obligation for the Member States to ensure the effectiveness of DPAs. This obligation will remain with the Member States, after the entry into force of the General Data Protection Regulation, however subject to precise parameters set by EU law.

Effectiveness is also reflected in the working methods of the relatively small DPAs. They are free to set their own agenda, but with one limitation, namely the hearing of complaints. The obligation of a DPA to handle a complaint is the subject of the pending case \textit{Rease and Wullems}.\textsuperscript{2660} This is an important case, because the nature of the obligation of the DPAs to handle complaints has a direct impact on their effectiveness, particularly in case the DPA were required to conduct an investigation into each complaint they receive.

\textit{Final recommendation}

This study proposes that a model for good governance for data protection authorities be developed. This model is inspired by the LITER Good Agency Principles,\textsuperscript{2661} which are aimed at making agencies work better. It should include the following elements:

- DPAs should, in the course of all their actions, protect their own independence and ensure that they do not take any external instruction.
- DPAs should effectively operate in between the EU level and the Member States, emphasising ‘proximity’ to the individual in their working methods.
- DPAs should demonstrate the results of past performance (accountability \textit{ex post}), by reporting in a public manner, and allowing public debate. This obligation should be

\textsuperscript{2658} For instance, the Dutch DPA will be, as from 2016, empowered to impose administrative fines with a maximum of 810,000 euros; see in Dutch: Staatsblad 230 Wijziging van de Wet bescherming persoonsgegevens, 2015.

\textsuperscript{2659} With the nuances in the case law of the CJEU, particularly in Cases C-131/12, \textit{Google Spain and Google Inc.}, EU:C:2014:317 and C-230/14, \textit{Weltimmo}, ECLI:EU:C:2015:639.

\textsuperscript{2660} Case C-192/15, \textit{Rease and Wullems}, pending. After the finalisation of the research it was reported that the case was withdrawn. However, in the near future similar questions may be raised before the Court of Justice.

\textsuperscript{2661} A. Ottow, Market & Competition Authorities, Good Agency Principles (Oxford University Press, 2015), mainly Chapter 3. See above Chapter 7, sections 7 and 15.
exercised without prejudice to the complete independence they enjoy vis-à-vis elected bodies.

- Transparency is a factor determining accountability during the process. Transparent working methods – such as peer reviews and impact assessments – could be instrumental in this context.
- Guarantees must be included in appointment procedures, involving different branches of government.
- The principle of sincere cooperation governs the cooperation of DPAs not only with EU bodies, but also with each other. DPAs should invest in cooperation in extraterritorial investigations.
- Under the principle of sincere cooperation, the DPAs are also encouraged to cooperate with EU agencies and national regulatory authorities with competences in other policy areas.
- Cooperation with the private sector is encouraged, but subject to the condition that responsibilities are not blurred.
- As public authorities DPAs should ensure that they include other public interests in their decision-making. Besides basing their assessment on the legal provisions on data protection, they should also take account of the wider context.
- Data protection law (for example, Directive 95/46) assumes that DPAs also have advisory tasks, which may conflict with their role as supervisor as envisaged by the Treaties. This conflict raises two issues:
  - It must be ensured that DPAs supervise compliance with legislation in an objective manner, even after having criticised this legislation in the legislative process;
  - In ‘accountability’ schemes, the supervisor must not become co-responsible for solutions at an individual level.
- Implementing and delegated acts (Articles 290 and 291 TFEU) should not be used as instruments by the Commission to make DPAs comply with changing views in society. Giving guidance to DPAs should be a task solely for the Article 29 Working Party, the institutionalised network of DPAs.

8. **Cooperation as an Element of Control, with a Layered Structure of Cooperation Mechanisms**

**Article 16(2) TFEU and the strengthened cooperation mechanisms under the GDPR (the first component)**

Cooperation of DPAs is an essential part of the control by DPAs. The mandate of DPAs comprises the obligation to contribute to a harmonised and effective level of data protection within the wider territory of the European Union. This is particularly important in an internet environment where dealing with cross-border effects is an inherent element of the protection that must be provided. Moreover, this obligation for DPAs is the consequence of the recognition that the Union is the appropriate platform for dealing with internet privacy and
data protection. In the light of these circumstances, enforcement has also become an EU concern.

DPAs should contribute to the control of data protection outside of the territory of their constituent Member State, mutually cooperating with their peers across the border. The duty for ensuring control in a cross-border context and for mutual cooperation follows from the system of EU law. Mutual enforcement cooperation consists of exchange of information, effectively assisting in supervision and – after the entry into force of the General Data Protection Regulation – the carrying out of joint investigative tasks, joint enforcement measures and other joint operations.

At present, the further task of contributing to a harmonised and effective level of data protection within the wider territory of the European Union is mainly a task for the Article 29 Working Party. The Working Party gives non-binding guidance, indirectly, yet significantly, influencing the supervision by the DPAs.

The General Data Protection Regulation brings two novelties. It introduces a one-stop shop mechanism with a lead supervisory authority cooperating with its peers in cases where DPAs in more than one Member State are concerned. The involvement of all concerned DPAs must ensure that in a single case only one decision is taken and, at the same time, prevent that multinational companies have to deal with divergent enforcement decisions. The system must also ensure that these companies only have to deal with one sole interlocutor. Under the consistency mechanism the EDPB, the successor of the Article 29 Working Party, will have a formal role in enforcement. In the view of the Commission, this mechanism serves as a conflict-solving mechanism between concerned DPAs and also as a mechanism to ensure the correct and consistent application of the regulation within the wider territory of the European Union. Other contributors to the legislative process consider that the role of the mechanism is limited to being a conflict-solving mechanism. This study concurs with the wide approach of the Commission.

The constitutional safeguards under EU law: cooperation mechanisms of DPAs, legal requirements for cooperation and a cooperation structure (the second component)

The Court of Justice’s case law on the independence of DPAs\(^{2662}\) directly affects the cooperation mechanisms of DPAs under Article 16(1) TFEU. Cooperation mechanisms should respect the independence of the participating DPAs or, alternatively, a cooperation mechanism having sufficient powers itself may become a DPA, subject to the requirements of independence in the Court’s case law.

Furthermore, the principle of sincere cooperation under Article 4(3) TEU applies to all governmental actors (EU and national) involved in the implementation of EU law and policies. This principle acquires an additional dimension in a composite administration where

cooperation between the different actors and levels is a condition for success. The principle of sincere cooperation extends to cooperation with authorities in related policy areas. Cooperation in the domain of privacy and data protection on the internet also involves non-governmental stakeholders. Where DPAs cooperate with actors outside government, the latter should respect principles of good governance, but Article 4(3) TEU does not apply to non-governmental stakeholders.

Administrative cooperation under EU law is a matter of common interest. Rules on administrative procedure should ensure the effective discharge of public duties and the protection of individuals’ rights. Arguably, in the light of the fundamental right of an individual to a good administration, as laid down in Article 41 Charter, the DPA cooperation should meet both objectives. The structure of DPA cooperation should not compromise the independence of DPAs and should equally not result in an incomplete – or extremely complex – system of remedies, in breach of Article 47 Charter.

Procedural guarantees – such as those included in the ReNEUAL Model Rules on EU Administrative Procedure – could deal with the disadvantages of fragmentation of administrative law in the European Union, also in the field of privacy and data protection. These guarantees could empower the individual to invoke his or her rights, in cases where a DPA hears a complaint, but lacks capacity to take an effective decision because of the cross-border nature of the case.

The next topic concerns the need for structures for cooperation to respect the constitutional safeguards under EU law. DPAs operating in multiple jurisdictions create a further challenge for reconciling independence, effectiveness and accountability. This study distinguished three models of cooperation: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models are examples of the integrated or composite EU administration where competences are not divided but shared. The main differences between these three models relate to the nature of coordination.

This study presented these three models as part of a layered structure for an independent, effective and accountable control of EU data protection. This layered structure should guarantee that the two objectives of cooperation of DPAs are satisfied: the protection of individuals vis-à-vis entities established outside the national territory, as well as the uniform interpretation of EU data protection law. The EDPB, as will be set up under the General Data Protection Regulation, should function both as a structured network and as a European DPA.

The added value of this layered structure is, in the first place, to clearly define where cases could be handled in the first layer, horizontal cooperation. If a case concerns data subjects in a large number of Member States, normally, horizontal cooperation would not be sufficient.

In the second place, this structure makes it possible to distinguish between the activities of the EDPB in a consistent manner, whilst reconciling legitimacy and effectiveness.

**Legitimacy as a factor for success for cooperation mechanisms (the third component)**

This study understood legitimacy in relation to the governance of privacy and data protection under EU law as meaning that some degree of accountability towards political institutions is ensured. Legitimacy as a factor for success of DPA cooperation requires *a priori* a degree of accountability vis-à-vis the political institutions of the Member States. Fundamental rights protection is a subject that is close to the citizen – the notion of proximity has been mentioned in this context – and this study also explained the perceived democratic deficit of the European Union. The cooperation by DPAs also requires transparency, in order to ensure some degree of accountability to the public.

Horizontal cooperation of DPAs is an expression of legitimacy in which the emphasis is on democratic accountability – political as well as public – at Member States level. Horizontal cooperation is characterised by the sharing of responsibilities, a common interest, good faith and good administration in the absence of hierarchy. Horizontal cooperation is not limited to two DPAs, but relates to all DPAs concerned. Where goods or services are offered on the internet, this can be the DPAs of all 28 Member States. Horizontal DPA cooperation requires specifying procedural guarantees, in order to facilitate the cooperation and to further ensure the guarantees at EU level.

The cooperation of DPAs as expert bodies should also enhance the uniform application of EU data protection law within the European Union. The cooperation mechanisms give effect to the task of DPAs to contribute to the control in the entire European Union, but they are also an expression of democratic legitimacy, because DPAs are situated in the Member States, close to the citizen.

This study argued that a structured network of DPAs – at present, essentially the Article 29 Working Party - is also primarily an expression of legitimacy, leaving the democratic accountability to a large extent at the national level. The structured network of DPAs will normally be strengthened with the setting up of the EDPB. In the exercise of its advisory role, giving guidance to DPAs as well as to the EU institutions, the EDPB will act as structured network.

The increased duties and powers of the network in the EDPB will enhance the requirements for its composition and for decision-making structures. In this context, this study emphasised the composition of the EDPB by senior representatives of DPAs as well as decision-making procedures based on consensus. A close relationship between the Commission and the EDPB as a structured network is desirable from the perspective of consistency, but direct influence of the Commission on the decision-making process should be avoided. A structured network requires procedural rules.
Increased duties and powers set higher standards for the independence of the EDPB, including a higher level of procedural guarantees and stronger requirements concerning the participation by the DPAs. Increased duties and powers also have an impact on the public and political accountability of DPAs. The European dimension of the activities of the DPAs and – even more – of the structured network of DPAs does not only require involvement of national parliaments, but also of the European Parliament.

**Effectiveness as a factor for success for cooperation mechanisms (the fourth component)**

This study specified the general principle of effectiveness under EU law as ensuring privacy and data protection by bridging the gap between principles and practice. Arguably, the contribution to the effectiveness of ensuring privacy and data protection is the main *raison d’être* for cooperation mechanisms.

Where goods or services are offered on the internet, horizontal cooperation may require the involvement of the DPAs of all 28 Member States. Hence, horizontal cooperation is not always effective. Neither is a structured network – with special responsibilities remaining with the national DPAs – sufficiently effective in all circumstances.

Effectiveness of enforcement by DPAs requires a strong cooperation mechanism that is able to deal with the challenges on the internet with big data, mass surveillance and loose governance structures. *A priori*, a strong European dimension in enforcement enhances the effectiveness, particularly the enforcement vis-à-vis big internet players. In addition, the mechanism itself should contain incentives for effective protection. For example, the effective implementation by the individual DPAs of the recommendations of the cooperation mechanism should be ensured. At the same time, there should be a system for monitoring the effectiveness of the cooperation mechanism itself.

Cooperation within a European DPA is an expression of effectiveness. It is expected that the EDPB will have certain – binding – powers to ensure compliance with data protection rules. Hence, when the EDPB exercises these powers, it becomes a DPA and should fulfil the conditions of independence under the Court of Justice’s case law.

Where the EDPB exercises binding powers, one may assume that a decision of the EDPB can be challenged before the Court of Justice, in accordance with Article 263 TFEU.

To the extent the EDPB acts as a European DPA, with decision-making power, it must meet higher standards of independence increase. The EDPB should be bound by the same standards of independence as national DPAs and procedural guarantees, comparable to the ReNEUAL Model Rules on EU Administrative Procedure,2664 are required. Moreover, the EDPB, acting as a DPA, should have the possibility to deliberate in enforcement cases.

---

without a European Commission representative being present. The system of redress must be sufficiently coherent and clear. Proximity, in the sense that an individual is entitled to redress in the Member State where he or she resides, is not a prerequisite for legal protection under EU law.

Where the EDPB acts as a European DPA, the involvement of the European Parliament as the body ensuring some degree of political accountability is obvious. The EDPB acts as an EU body. However, the EDPB – which is largely composed of national DPAs – should also incite involvement from national parliaments. This is a further illustration of the complex relationship between control under Article 16(2) TFEU and the public and political accountability.

**Final recommendation**

This study presented three models of cooperation: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models compose a layered structure for an independent, effective and accountable control of EU data protection.

At present, the control of the compliance with data protection rules is not centralised at the EU level. Although considerations of effectiveness plead in favour of a uniform and harmonised approach of the control, this does not mean that centralisation of control would be the preferred option, at least not in the immediate future. Centralisation of control is also not favoured in any of the contributions of the EU institutions to the legislative process in the General Data Protection Regulation.

The study recommended elaborating the layered structure, as a structure for better governance of control of data privacy and data protection in the European Union. This layered structure is not meant to centralise essential parts of the decision-making by DPAs at the European level, but to ensure that where the European level is involved in the control of data protection rules, appropriate standards are in place.

9. **External EU Action on the Internet: Solving Conflicting Jurisdictional Claims and Substantive Divergences, with a Powerful EU in the International Domain**

**Article 16 TFEU and the claim of extraterritorial jurisdiction (the first component)**

As a rule, any intervention by the European Union with the purpose of protecting privacy and data protection on the internet has extraterritorial effect. In addition, giving extraterritorial effect to EU data protection law is an explicit objective of the EU legislator, resulting from the general ambitions of the Union to promote its essential values, also in the wider world. A further point of departure for the Union’s role in the external domain is that, due to the
pervasiveness of the internet in our daily lives, the internet should not be governed by a separate body of law.

The global nature of the internet requires that in the external domain solutions should be found for two types of issues: conflicting jurisdictional claims and divergences in substantive law. The study proposes an active role of the European Union in the external domain, based on an appropriate mix of different strategies, and addressing both types of issues.

The overlapping of jurisdictions is no longer an exception on the internet. Under public international law, there is no generally accepted solution for internet jurisdiction. General public international law implies that states (and the European Union) are precluded from enforcing their laws in another state’s territory. However, states may prescribe rules for persons and events outside their borders. In accordance with public international law, the European Union – acting as if it were a state – should claim extraterritorial jurisdiction, even if it lacks enforcement power, for instance to stimulate voluntary compliance in third countries.

The constitutional safeguards under EU law where the EU acts as an organisation sui generis in the external domain (the second component)

The European Union itself is an organisation sui generis, also in the international domain. International competence of the European Union, under international law, is similar but not equal to that enjoyed by a state. The European Union is not a member of international organisations such as the UN, the OECD and the Council of Europe. It must be assumed that the Union has, under Article 16 TFEU, exclusive competence in respect of the external dimension of data protection, because effective protection on the internet requires the widest possible geographical scope. Arguably, the Member States lost their external competence in the domain of privacy and data protection. In any event, the Member States are expected to lose their external competence after the entry into force of the General Data Protection Regulation, at least in the areas covered by this instrument.

Where the European Union uses its external competence, it acts under international law. The Court of Justice determines the limits of the Union’s external competence and of the primacy of international law in the EU legal order. It is the Court itself that ultimately – and in last resort exclusively – interprets the Charter and, more generally, EU law. Provisions of international agreements have direct effect within the EU legal order, but subject to the nuance that international law cannot have the effect of prejudicing the constitutional principles of the Treaties (the Kadi case law).2665

The qualification of DPAs as new branches of government also has institutional consequences in the external domain. In the areas of their competence, the DPAs represent the European Union externally. However, they must respect the consistency of external EU policy. The principle of sincere cooperation binds the DPAs, but also commits the EU

2665 Mainly, Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461.
institutions to involve the DPAs where they take positions in the external domain on policies touching upon privacy and data protection, for instance in negotiations with third countries in this area, conducted according to the procedure of Article 218 TFEU. DPAs should not commit the European Union to international obligations, but they are empowered to engage in enforcement arrangements.

This brings us to the external strategies in the light of the constitutional safeguards under EU law. This study distinguishes three strategies for the European Union operating in the external domain: a unilateral, a bilateral and a multilateral strategy. The unilateral strategy basically means exporting the EU standards. The bilateral strategy involves seeking arrangements with relevant, like-minded jurisdictions such as the US and, by doing so, building bridges between these jurisdictions. The multilateral strategy aims at developing global standards.

These strategies should deal with the two types of issues mentioned above: conflicting jurisdictional claims and divergences in substantive law. Reconciling legitimacy and effectiveness means in relation to jurisdictional claims: ensuring effective protection of individuals in the European Union and, at the same time, basing the legitimate claim of jurisdiction on the internet on a meaningful link with the Union. Divergences in substantive laws could be addressed by allowing practical arrangements with third countries and international organisations at an effective level of protection, but not by lowering the legitimate level of protection of individuals in the European Union.

Legitimacy as a factor for success for the EU acting in the external domain (the third component)

The relationship between the European Union and the jurisdictions of third countries and international organisations is one of the main complicating factors of effective internet regulation, also from a perspective of legitimacy. The legitimacy of external EU action is also affected by – possibly conflicting – legitimate claims of third countries and international organisations.

In the external relations with third countries, the relationship with the United States plays an important role. An important element of the controversy between the EU and the US is a difference in approach between the two jurisdictions. The approach of the US – at least in relation to consumer privacy – does not aim at giving wide territorial scope to US law, but at increasing interoperability between privacy laws by pursuing mutual recognition. In contrast, the fact that privacy and data protection have the status of fundamental rights under EU law prevents the mutual recognition of substantive principles of EU law in this area, if the standards in a third country do not comply with the Charter.

Two of the most relevant international organisations for the European Union are the United Nations and the OECD. Under current law, the UN does not impose any obligation on the EU. However, the EU should encourage the UN to play a more prominent role. The OECD guidelines emphasise the need for improved interoperability of privacy frameworks and for
cross-border cooperation between privacy enforcement authorities. The OECD is a suitable forum for discussion with the US.

The closest ally of the European Union in the field of data protection is the Council of Europe, which provided inspiration for privacy and data protection in the Union, through the case law of the European Court of Human Rights and through Convention 108. Institutionally it is a difficult relationship, as may be illustrated by the negative Opinion of the EU Court of Justice on the draft accession agreement on the accession of the Union to the ECHR, as provided for in Article 6 TEU. An example in the domain of privacy and data protection illustrates the difficult relationship: ratification by a third country of Convention 108 – meaning compliance with the Convention – does not guarantee that a third country is considered as providing adequate protection under Directive 95/46 making it possible that personal data are transferred to this third country without further safeguards.

A legitimate claim to external EU jurisdiction in the area of privacy and data protection should be based on a meaningful link with the effective protection of the individual in the European Union. This meaningful link with the Union could consist of personal jurisdiction based on residence and the doctrine of effect. The study suggests that the Union should promote this foundation of – personal – jurisdiction in the international context. This suggestion does not aim at solving the problem of internet jurisdiction, but could be included in the external EU action in the area of privacy and data protection.

The European Union should, also in the external domain, respect some degree of accountability towards political institutions. This accountability has a connection with the democratically agreed substantive level of privacy and protection, as laid down in the EU rules under Article 16(2) TFEU. Where the Union acts in the external domain, individuals may have the legitimate expectation that this will not lower the – legitimate – level of protection of individuals in the European Union.  

Effectiveness as a factor for success for the EU acting in the external domain (the fourth component)

Effectiveness is even more decisive as a factor in the external domain than it is in the internal domain. The perceived loss of control is closely related to the fact that many data controllers have their establishment outside EU territory and that personal data of individuals in the European Union are available all over the globe. Effectiveness is the factor for success. This justifies explaining three strategies for external action of the Union in the light of the effectiveness of the EU action.

---


2667 This is illustrated by Case C-362/14, Schrems, ECLI:EU:C:2015:650, where this expectation was not met and hence a Commission Decision was declared invalid.
The unilateral strategy – which basically means exporting the EU standards – is a potentially successful approach, if it is based on the conditions of Bradford, which are summarised as the “Brussels effect”2668. The European Union has regulatory clout, manages to set the global standards for regulation on privacy and data protection and is capable of ‘exporting’ its system on privacy and data protection and of assuming leadership in global regulation. This strategy enables the building of alliances on a practical level with like-minded countries, based on common challenges in the field of internet privacy.

This study explained the bilateral strategy as an approach through which the European Union seeks to conclude arrangements with relevant, like-minded jurisdictions such as the US and, by doing so, to build bridges between these jurisdictions. A bilateral agreement on privacy and data protection between the EU and the US, based on reciprocity, would be something new.2669 An agreement does not necessarily mean an approximation of standards of privacy and data protection, which could be difficult to align with the Charter, but could also focus on mutual recognition, standardisation processes or enforcement cooperation.

The multilateral strategy aims at developing global standards. The European Union should strive for global rules, most logically within the framework of the United Nations. The multilateral strategy is rather a long shot, but a multilateral, global agreement, would in the long term, be the most appropriate instrument for effectively ensuring privacy and data protection on a global scale. Such an agreement would not necessarily include an approximation of standards, but it could also focus on mutual recognition, standardisation processes or enforcement cooperation.

The contributions of the actors and roles indicated in Article 16 TFEU demonstrate that in practice the unilateral strategy is most important.

In *Google Spain and Google Inc*, the Court of Justice contributed to the unilateral strategy under Article 16 TFEU, by highlighting the effectiveness of the protection of Europeans and by requiring a meaningful link with the European Union. The Court did not address the impact of its ruling on competing jurisdictions on the internet. The ruling in *Schrems*2670 on the Safe Harbour Agreement with the US2671 was the first opportunity for the Court to clarify the essential requirements for bilateral and multilateral agreements, affecting the protection of individuals within the Union. A second opportunity will present itself with the Opinion on the agreement with Canada on passenger name record data2672.

---

2669 Possibly, with the exception of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses (“Umbrella Agreement”), which is, at present, in a final stage of negotiations.
2670 Case C-362/14, Schrems, ECLI:EU:C:2015:650.
2672 Opinion 1/15 (pending) on Agreement between Canada and the European Union on the transfer and processing of passenger name record data
The EU legislator gives wide external effect to EU law on data protection, with the unilateral approach as a composing element and the regime of data transfers as a typical example. Article 43a of the proposed General Data Protection Regulation\textsuperscript{2673} is a unilateral solution for a conflict of law. Promising bilateral or multilateral strategies include methods to ensure the interoperability between different legal systems, without necessarily adapting the level of protection in other regions of the world to the EU level, nor lowering the level of protection in the European Union.

For the DPAs and the cooperation between DPAs the starting point is a unilateral strategy: the task of the authorities is to control EU law. The cooperation between DPAs and regulatory agencies in third countries is an exponent of the bilateral and multilateral strategy. Bilateral Memoranda of Understanding between European DPAs and the Federal Trade Commission\textsuperscript{2674} and multilateral cooperation in the Global Privacy Enforcement Network (GPEN)\textsuperscript{2675} are examples. It is an omission that the General Data Protection Regulation does not include rules on enforcement cooperation with authorities of third countries and with international organisations.

\textit{Final recommendation}

The European Union emphasises the need for taking responsibility for globalisation, claiming that its values have a normative strength and are universally applicable. The Union has global power through the legal standards representing these values.

In order to ensure effective protection of individuals on the internet, the preferred strategy should be the unilateral strategy, aiming at exporting EU values in the international domain. The European Union could thereby use facilities offered by the Council of Europe, such as the possibility of non-European countries adhering to Convention 108. As part of this strategy, on a practical level, bridges should be built with like-minded countries.

In addition, the bilateral strategy should be explored, focusing on mutual recognition, standardisation processes or enforcement cooperation, based on the communality between the systems, but also accepting the differences. The OECD could possibly play a role.

In the long term, a UN Treaty would ensure the best protection (the multilateral approach). The European Union should take initiatives in order to facilitate the adoption of such a Treaty, with the ambition to achieve a minimum standard of data protection.

\textit{10. The Prospect of a GDPR}

\textsuperscript{2673} Consolidated text (outcome of the trilogue of 15/12/2015), available on http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884.#.
\textsuperscript{2674} The DPAs in Ireland, the UK and The Netherlands cooperate with the FTC on the basis of these memoranda, see Chapter 9, Section 17.
\textsuperscript{2675} See: https://www.privacyenforcement.net.
This study was based on the present state of EU data protection law. This final chapter ends with a short outlook towards future EU law on data protection, by expressing some expectations in respect of the governance model under Article 16 TFEU following the data protection reform, particularly the General Data Protection Regulation. These observations will remain general, to avoid becoming speculative, also because at the time of writing much was still unclear about the final outcome of legislative texts and about the application of these texts in practice.

The subject of this study was Article 16 TFEU. The study gave an analysis of the mandate under Article 16 TFEU. The study analysed neither Directive 95/46, nor any other legislative instrument of the European Union in the area of privacy and data protection. Of course, Article 16 TFEU cannot be analysed in isolation and the study regularly referred to Directive 95/46, and sometimes to other legislative instruments on data protection.

These considerations explain why this study does not include an assessment of the General Data Protection Regulation, nor of the proposed directive for data protection in the police and judicial sectors on the basis of the latest available texts. At several places the study includes references to the General Data Protection Regulation and sometimes to the proposed directive, as an illustration of points made.

The General Data Protection Regulation contains elements designed to significantly change the governance of EU privacy and data protection, not the least of which is the changed legal instrument, with a regulation replacing a directive as the core instrument. The provisions in the General Data Protection Regulation have an impact on the exercise of the various roles under Article 16 TFEU. The regulation is designed to contribute to the effective and legitimate exercise of the mandate of the European Union, enabling the actors under Article 16 TFEU to contribute to the fulfilment of this mandate in a successful manner.

The state of play in the legislative process

On 25 January 2012, the Commission adopted its proposal for a General Data Protection Regulation, together with a proposal for a directive for data protection in the police and judicial sectors, and a Communication explaining the data protection reform, as a package. These documents followed wide consultations with interested parties lasting for

---


2679 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.
over two years. The European Data Protection Supervisor had already called for a reform of the legislative framework in July 2007.

On 12 March 2014, the European Parliament adopted a legislative resolution on the proposed regulation, in which it proposes 207 amendments on the recitals and articles of the Commission proposal. These 207 amendments are a synthesis of more than 4000 proposals for amendments submitted by Members of the European Parliament. On the same date, the European Parliament adopted a legislative resolution on the proposal for a directive for data protection in the police and judicial sectors.

On 15 June 2015, the Council of the European Union adopted a general approach on the proposed regulation, but not yet on the proposed directive. In this general approach, the Council submits a fully revised text of the Commission proposal. On the basis of these three documents, the informal triilogue was taking place in which the European Parliament, the Council and the Commission participated. This led to an outcome and must lead to formal adoption in the first half of 2016.

These trilogues, not mentioned in Article 294 TFEU, which outlines the ordinary legislative procedure under EU law, are usually conducted in a non-transparent manner. The objective is to reach an agreement on the text that enables the adoption of the regulation under what Article 294 TFEU calls “the first reading”. The TFEU lays down formally that “if the Council approves the European Parliament’s position, the act concerned shall be adopted in the wording that corresponds to the position of the European Parliament”. In practice, the agreement between the institutions is laid down in a position of the European Parliament and subsequently approved by the Council.

This state of play demonstrates the complexity of the process and is a confirmation of what was said earlier in this study, namely that legislation requires reflection and thus time,

---

2685 For an overview of the different texts, see the Annex (also available as app) of European Data Protection Supervisor, Opinion of 27 July 2015 - Europe’s big opportunity, EDPS recommendations on the EU’s options for data protection reform.
2687 As referred to in Chapter 4, Section 10.
2688 Article 294(4) TFEU.
2689 In Chapter 6.
whereas in the information society technologies change with a rapid pace. At the same time, this state of play reflects the determination of the Commission, the European Parliament and the Council to come to a result.

**General Remarks on the GDPR, on Effectiveness and Legitimacy**

The debate on the proposed General Data Protection Regulation was largely dominated by arguments relating to efficiency and effectiveness. The Commission motivates its proposal on the basis of these arguments. The Explanatory memorandum underlines that the “current framework remains sound as far as its objectives and principles are concerned”. A new framework is needed for other reasons. It should be stronger than the present one, more coherent and backed by strong enforcement, just to mention a few catchwords used in the Explanatory memorandum.  

An essential impetus for the reform is the empowerment of the individual, the data controller and the data protection authorities, as is clear from the two communications of the Commission explaining the reform. Other documents contributing to the legislative procedure, too, emphasise the need for improving the effectiveness of data protection in the European Union. An example is the Opinion of the European Data Protection Supervisor of 27 July 2015, which underlines the need for the empowerment of the individual and for the strengthening of the responsibilities of businesses and public authorities.

However, these are not the only arguments in the debate. Legitimacy also plays a role in the discussion in the legislative process. An example is the discussion on the tasks of the independent data protection authorities and their cooperation within a one-stop shop mechanism. Several arguments have been put forward, relating to ‘proximity’ to ensure that the primary responsibility for protection remains with the national DPAs. The consistency mechanism with involvement of the EDPB should only be triggered “where it is necessary”. In addition, the mechanism “should not encroach upon the independence of national supervisory authorities and should leave the responsibilities of the different actors”.

---


2691 See the references to empowerment or strengthening the control in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM (2012) 9 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final.

2692 “Effective data protection empowers the individual and galvanises responsible businesses and public authorities”; European Data Protection Supervisor, Opinion of 27 July 2015 - Europe’s big opportunity, EDPS recommendations on the EU’s options for data protection reform, at 2.

2693 E.g., by the French DPA (CNIL); Raynal in Carine Dartiguepeyrou (ed.), The Futures of Privacy, Cahier de prospective, Think Tank Futur Numérique, at 72.

2694 As explained in Chapter 8, Section 12 of this study.

Another topic in the discussion is the need for flexibility for the Member States, to complement and possibly even derogate from the regulation, also in view of the democratic legitimacy. The concern of the Member States inspired the Council to propose a new Article 2a for the regulation, allowing Member States to specify the regulation for the public sector or for data processing “for compliance with a legal obligation or for the performance of a task carried out in the public interest”. This provision did not survive the trilogues, but some leeway is given to the Member States in a new Article 6(2a).

Observations on the ambitions of the GDPR to ensure a successful exercise of the roles under Article 16 TFEU

The General Data Protection Regulation implements the mandate under Article 16 TFEU, in principle, in a comprehensive manner, although Article 2(2) of the Commission proposal excludes certain areas from its scope.

First, the General Data Protection Regulation will change the conditions for a successful exercise of the mandate under Article 16 TFEU in a significant manner. The chosen instrument – a regulation, with general application, binding in its entirety and directly applicable in all Member States – significantly limits the margin of discretion of the Member States. The Member States will have to repeal their national data protection laws. The General Data Protection Regulation will centralise the governance of data protection to a large extent at the EU level. This is a significant change in the exercise of the role of the EU legislator. However, a successful use of the EU mandate will also require that in this domain of fundamental rights the Member States continue to play a role. The effects of the General Data Protection Regulation on the Member States are not obvious. It will delegate certain roles to the Member States, but its effect on the relationship between the two levels in privacy and data protection and related areas is, at this stage, not fully clear.

Second, the General Data Protection Regulation will have an impact on the conditions for a successful exercise of the role of the Court of Justice’s mandate under Article 16(1) TFEU. The proposed regulation has a strong focus on improving governance and will not fundamentally change the main principles of data protection, although some changes have been proposed. However, the regulation will not only have an impact on the possibilities to protect the fundamental right to data protection within the national jurisdiction, but also on the possibilities of Member States to protect the rights coinciding with it, such as the freedom of expression, and public interests.

---

2696 Preparation of a general approach, Note from Presidency to Council, 11 June 2015, 9565/15.
2698 In particular the areas covered by the directive in the police and judicial sectors and the processing by EU institutions, bodies, offices and agencies; see Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
2699 Article 288 TFEU.
Privacy and data protection are regulated by EU law, whereas other fundamental rights – and the public interest of security – are mainly a concern for the Member States. This may impact the balancing in a significant manner, for instance regarding the relationship with the freedom of expression which is left to the Member States, under Article 80 of the Regulation.\textsuperscript{2700}

Third, the choice of instrument as well as the substance of a number of provisions in the General Data Protection Regulation will have – as was mentioned above – a centralising effect on the governance of privacy and data protection and lead to an expansion of the role of the EU legislator. On the one hand, the proposed regulation centralises, but, on the other hand, it will also have a strong focus on the involvement of other governmental and nongovernmental stakeholders. The regulation will contain provisions detailing the involvement of the private sector, provisions relating to independent supervisory authorities and the cooperation between these authorities, and provisions on the external aspects of the General Data Protection Regulation, defining the relationship between the European Union and third countries and international organisations.

A further change is that the General Data Protection Regulation will introduce or reinforce arrangements with the purpose of improving the governance of privacy and data protection and, at the same time, bridging the gap between principles and practice. Accountability is an alternative for command-and-control legislation, based on general notions of the quality of legislation. Privacy by Design should enhance trust in data protection and at the same time create economic incentives.

Fourth, the provisions in the General Data Protection Regulation relating to independent supervisory authorities are expected to bring a significant change. These provisions centralise the main conditions for the functioning of these authorities at the European level. These provisions also address the presumed weaknesses in the powers and resources of the DPAs, for instance by attributing strong sanctioning powers to the DPAs.

Fifth, the General Data Protection Regulation will significantly change the cooperation mechanisms of DPAs. The regulation will create a one-stop shop mechanism with a lead supervisory authority cooperating with its peers, and a consistency mechanism giving the EDPB a formal role in enforcement. This new structure recognises that horizontal enforcement cooperation between DPAs is not sufficient, and that a European body should play a role in the enforcement. The structure will not distinguish between the various roles of the EDPB. The EDPB, as proposed in the regulation, could function both as a structured network and as a European DPA. However, the requirements for the functioning of the EDPB are different, depending on the function.

Sixth, the provisions of the General Data Protection Regulation dealing with the external effect of EU data protection law should improve the protection of individuals in the Union, in situations not confined within the territory of the European Union. The regulation underlines

\textsuperscript{2700} The Council, e.g., proposes to leave the task of balancing to national law; Article 80 of Preparation of a general approach, Note from Presidency to Council, 11 June 2015, 9565/15.
that the offering of goods or services to data subjects in the Union and the monitoring of these data subjects falls within its scope.\textsuperscript{2701} Also, the rules on transfers of personal data to third countries will be modernised, for instance by creating an explicit legal basis for transfers by way of binding corporate rules.\textsuperscript{2702} However, the entry into force of the regulation itself may be the most important development for the external action of the Union. An EU with a modern and effective regime for privacy and data protection is expected to give it more leverage in the international domain than an EU that can be criticised because of the imperfections of its internal legal framework.

\section*{11. Final Conclusions}

The success of the European Union in exercising its mandate under Article 16 TFEU is essential for individuals whose fundamental rights are at stake. It is also essential for our democracies, which are subject to the rule of law. Moreover, if the Union can successfully realise its ambitions under Article 16 TFEU and is capable of effectively contributing to the respect of the rights to privacy and data protection, this will give legitimacy to the mandate under the same article and, in a wider context, raise trust in the European Union (and indirectly, in national governments).

The perspective of this study is optimistic. Under Article 16 TFEU, the European Union has an appropriate mandate to act in the area of privacy and data protection, with tasks attributed to the judiciary, the EU legislator and the independent data protection authorities, in principle without restrictions. The mandate also enables a successful cooperation between the data protection authorities and for the European Union as such to operate in the international domain. This optimistic perspective is also based on the strong position of Europe in the international domain, based on what has been called the “Brussels effect”\textsuperscript{2703} Law can make a difference in an information society provided that the available instruments are used in an intelligent manner. Moreover, the European Union is capable of realising the objectives laid down in its general constitutional structure, and in particular in Article 16 TFEU.

The success of the European Union in the exercise of its mandate under Article 16 TFEU depends on the way the Union manages to reconcile the requirements of legitimacy and effectiveness. A successful exercise of the EU mandate in the domain of privacy and data protection could demonstrate the capabilities of the Union to protect fundamental rights in a global environment. This is a domain where not only law, but also the European Union, by exercising its mandate in a successful manner, can make a difference.

This study argues that Article 16 TFEU could benefit from an understanding of the fundamental rights to privacy and data protection as such and in their relation to other fundamental rights, which takes the changed environment of the internet into account. Since, in an internet environment, all processing of personal data potentially affects the privacy of

\textsuperscript{2701} Article 3(2) of Commission Proposal for a General Data Protection Regulation, COM (2012), 11 final.
an individual, it no longer makes sense to consider privacy and data protection as separate fundamental rights. On the contrary, these rights are part of one system. Moreover, on the internet, privacy and data protection, on the one hand, and other fundamental rights, on the other hand, increasing collide, whereas, at the same time, the protection of fundamental rights is becoming increasingly complicated. Against this background, a simple taxonomy of fundamental rights is proposed that makes it possible to differentiate in the level of protection, depending on the nature of the right.

The Court of Justice, in its case law, considers the need to compensate the perceived loss of control over personal data, enabled by the current legislative instruments on data protection and in particular Directive 95/46. The EU legislator is working towards the adoption of a comprehensive and up-to-date legislative framework for data protection that will introduce important innovations. The Treaties recognise the essential role of control by data protection authorities with a high degree of independence, as confirmed in the case law of the Court. The authorities and their cooperation structures play an essential role in the development of data protection in the European Union. This role will be further developed in the new legislative framework. Finally, the European Union plays an active role in the international arena, through the contributions of the various actors and roles under Article 16 TFEU.

This chapter started with an emphasis on what is at stake. The stakes are high for the European Union, in the exercise of its mandate of ensuring privacy and data protection on the internet. The challenges in the information society require ambitious approaches. This study demonstrates that the Union is showing ambitions in exercising its mandate under Article 16 TFEU. The study gives illustrations of how the various actors are contributing to the success of the fulfilment of the mandate. It provides recommendations for a successful exercise of the mandate, with the prospect that in the coming years the General Data Protection Regulation will become applicable.

The relevance of the findings in this study is not necessarily restricted to the area of privacy and data protection. The internet poses challenges for other areas of law as well. Moreover, the governance model in the field of data protection – with a key role of expert bodies in between the national and the European jurisdictions – has parallels in other areas of EU intervention.

For the short term, the General Data Protection Regulation means a significant step forward for data protection in the European Union, with relevance for all actors under Article 16 TFEU. The General Data Protection Regulation, however, does not solve all the weaknesses in the system. It remains to be seen whether, in the long term perspective, the regulation will suffice. Subjects that in any event require further action in the longer term are:

- The adaptation of the substantive principles of data protection;
- The fine-tuning of the role of the Member States under Article 16 TFEU;
- The centralisation of the supervision of global internet companies.

These subjects should be further explored in academic research in the coming years.
<table>
<thead>
<tr>
<th>European Union</th>
<th>Article 16 TFEU</th>
<th>Constitutional safeguards under EU law</th>
<th>Legitimacy</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Challenge:</strong> Compensate for lack of control on internet</td>
<td>Strong: The mandate</td>
<td>Strong: Exercise of mandate on internet gives effect to subsidiarity principle</td>
<td>Strong: Article 16 TFEU potentially increases legitimacy EU</td>
<td>Strong: Output, flexibility, bridging the gap by involving public actors</td>
</tr>
<tr>
<td><strong>Challenge:</strong></td>
<td></td>
<td>Challenge: Executive federalism and harmonisation</td>
<td>Challenge: Social legitimacy; reconcile with MS competence</td>
<td>Challenge: Involving private sector in appropriate way</td>
</tr>
</tbody>
</table>

| CJEU | Strong: Acting in disputes and as constitutional court | Strong: Ability of balancing with other interests | Strong: Compensation for democratic deficit | Strong: Effectiveness as main element of case law |
| **Challenge:** | Challenge: Incremental nature case law | Challenge: Adjudicating based on simple taxonomy | Challenge: Ensuring precise answers |

| EU legislator | Strong: The complete mandate | Strong: Regulation as the main instrument, also for public sector | Strong: Involvement of various actors in process | Strong: Regulation giving the right incentives for compliance |
| **Challenge:** Addressing the main principles of data protection | Challenge: Interfaces with other competences Ensure role MS | Challenge: Addressing synergies; develop strategy | Challenge: Improving accountability |

| DPAs | Strong: Constitutional embedding Variety of roles | Strong: Expert bodies In between Brussels and MS | Strong: Independence increases reliability Output legitimacy | Strong: Independence as guarantee for effective control |
| **Challenge:** Combine variety of roles | Challenge: Considering other fundamental rights and public interests | Challenge: Link with democratic bodies; work on basis of governance model | Challenge: Addressing deficiencies in powers and resources |

| Cooperation mechanisms of DPAs | Strong: Cooperation essential part control Combining national and EU interests | Strong: Sincere cooperation | Strong: Sharing, not dividing responsibilities Enables link with national jurisdiction | Strong: Cooperation mechanisms with European dimension |
| **Challenge:** Implement novelties GDPR | Challenge: Procedural guarantees; ensuring independence within cooperation | Challenge: Work on basis of layered structure | Challenge: Is GDPR ambitious enough? |

| **Challenge:** Overlapping of jurisdictions is the rule | Challenge: Enforcing EU law outside EU territory; how do DPAs represent the EU externally? | Challenge: Claims 3rd countries and int. organisations; combining unilateral, bilateral and multilateral strategies | Challenge: Compensate loss of control; protect in absence of global rules |
The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU

SHORT SUMMARY

The study was triggered by a perceived loss of control of governments over societal developments, due to globalization and technological developments, which inhibit the effective protection of essential values in democratic societies.

Privacy and data protection are essential values in democratic societies, which are subject to the rule of law. The EU Treaties have granted the Union a widely formulated role in ensuring effective protection of these fundamental rights of the individual, by means of judicial review, legislation and supervision by independent authorities. Hence, the imperative of protection is laid down at the constitutional level, empowering the Union to play its role as constitutional guardian of these two fundamental rights.

More precisely, Article 16 TFEU, read in connection with Articles 7 and 8 of the Charter of the Fundamental Rights of the Union, lays down the tasks of the EU in relation to privacy and data protection as fundamental rights for individuals. Article 16(1) TFEU and Articles 7 and 8 of the Charter specify the right to data protection which the EU should guarantee, ultimately under control of the Court of Justice, Article 16(2) TFEU empowers the EU legislator to set rules on data protection, and, finally, control should be ensured by independent authorities (under Article 16(2) TFEU and Article 8(3) Charter).

Article 16 TFEU gives the EU a specific mandate to ensure data protection, in addition to the general responsibility of the Union – and of the Member States where they act within the scope of EU law - to respect the fundamental rights laid down in the Charter. The Charter determines that where the EU acts, fundamental rights should be respected. Article 16 TFEU lays down that the EU shall act in order to ensure the fundamental right to data protection.

The mandate under Article 16 TFEU is broadly formulated and gives the Union – in principle – the power to act, and make a difference. This is a subject where the EU can act successfully, by addressing a problem with a global scale and which is technologically difficult.

This specific mandate of the EU in respect of privacy and data protection is the subject of this study. The study analyses the contributions of the specific actors and roles within the EU framework: the judiciary, the EU legislator, the independent supervisory authorities, the
cooperation mechanisms of these authorities, as well as the EU as actor in the external domain. The legitimacy and the effectiveness of the EU and of the operation of the actors and roles within the EU framework are important perspectives for this analysis.

General conclusions

This analysis shows that successful use of EU powers under Article 16 TFEU can be made, in conformity with the requirements of legitimacy and effectiveness. It also shows that ambitious approaches are needed, in view of the huge challenges in the information society.

The success of the EU in exercising its mandate under Article 16 TFEU is essential for individuals whose fundamental rights are at stake. It is also essential for our democracies which are subject to the rule of law. Moreover, if the Union can successfully deliver upon its ambitions under Article 16 TFEU and is capable to effectively contribute to the respect of the rights to privacy and data protection, this will give legitimacy to the mandate under the same article and in a wider context raise the trust in the EU (and indirectly, in national governments).

The perspective of this study is optimistic. The EU has an appropriate mandate to act in the area of privacy and data protection, with tasks attributed to the judiciary, the EU legislator and the independent data protection authorities, in principle without restrictions. The mandate also enables a successful cooperation of the data protection authorities and for the EU as such to operate in the international domain.

This optimistic perspective is also based on the strong position of Europe in the international domain, based on what has been called the “Brussels effect”. Law can make a difference in an information society provided that the available instruments are used in an intelligent manner. Moreover, the European Union is capable to deliver upon its ambitions laid down in its general constitutional structure, and in particular in Article 16 TFEU.

The success of the EU in the exercise of its mandate under Article 16 TFEU depends on the way the EU manages to reconcile the requirements of legitimacy and effectiveness. A successful exercise of the EU mandate in the domain of privacy and data protection could show the capabilities of the EU to protect fundamental rights in a global environment. This is a domain where not only law, but also the EU, by exercising its mandate in a successful manner, can make a difference.

This study argues that Article 16 TFEU could benefit from an understanding of the fundamental rights to privacy and data protection as such and in their relation to other fundamental rights which takes the changed environment of internet into account. Since, in an internet environment, all processing of personal data potentially affects the privacy of an individual, it makes no longer sense to consider privacy and data protection as separate fundamental rights. On the contrary, these rights are part of one system. Furthermore, the

right to data protection does not include a right to prohibit processing; on the contrary, it is a right to fairness.

Moreover, on the internet, privacy and data protection, on the one hand, and other fundamental rights, on the other hand, increasing collide, whereas, at the same time, the protection of fundamental rights becomes increasingly complicated. Against this background, a simple taxonomy of fundamental rights is proposed, enabling to differentiate in the level of protection, depending on the nature of the right.

The Court considers in its case law the need to compensate the perceived loss of control over personal data, enabled by the current legislative instruments on data protection and in particular Directive 95/46. The EU legislator works towards the adoption of a comprehensive and up to date legislative framework for data protection, bringing important innovations. The Treaties recognise the essential role of the control by data protection authorities with a high degree of independence, as confirmed in the case law of the Court. The authorities and their cooperation structures play an essential role in the development of data protection in the European Union. This role will be further developed in the new legislative framework. Finally, the EU plays an active role in the international arena, through the contributions of the various actors and roles under Article 16 TFEU.

Specific findings, focusing on the various actors and roles

Article 16 TFEU provides a strong mandate to the EU and ensures that privacy and data protection fall by definition within the scope of EU law. The high ambitions of the EU resulting from this mandate should compensate for the presumed lack of control on internet. The EU is not the sole guardian of privacy and data protection on the internet. Also the Member States have a role. The executive federalism should not adversely affect the harmonised level of protection.

An appropriate exercise of the mandate under Article 16 TFEU contributes to the EU’s social legitimacy and can also be an element of the enjoyment of EU citizenship. EU action should also be legitimate vis-à-vis the Member States. Effective exercise of the mandate gives the EU output-legitimacy. Bridging the gap between principles of privacy and data protection and practice requires an appropriate choice of legislative arrangements, strengthening the various (public) actors and roles under EU law, as well as involving the private sector and leaving the final responsibility with governmental actors.

This study includes a number of ideas on the involvement of the various public and private actors in the governance of internet privacy and data protection. The study recommends elaborating these ideas and developing a strategy for this involvement, clearly describing the responsibilities of the various actors.

In recent years, the Court of Justice played an important role in promoting privacy and data protection, also taking into account the impact of the information society. Two judgements in
2014, *Google Spain and Google Inc*, and *Digital Rights Ireland and Seitlinger* are the best illustrations of a court, taking privacy and data protection serious. The recent *Schrems* ruling confirms this line.

This study does the following recommendation, to base the scrutiny of fundamental rights in an internet environment on a simple taxonomy. This taxonomy of fundamental rights is structured as follows:

- **d.** Non-derogable or absolute fundamental rights, corresponding to the rights included in Title I of the Charter, entitled dignity;
- **e.** Rights with a huge impact on the human dignity, but not qualified as non-derogable, such as privacy and data protection;
- **f.** Social, cultural and economic rights. Further categories include: principles in the Charter (as meant in Article 51(1) and 52(5) thereof), the fundamental freedoms of the Treaties, relating to free movement, the undefined species of public and general interests.

As far as the **EU legislator** is concerned, the study mentions five directions for the EU and the Member States to regain control. First, the existing legal instruments for privacy and data protection should be interpreted in a way, taking the changed circumstances into consideration; second, the legislative arrangements should be adapted to the new circumstances; third, the changed relation between the public and the private sector should be addressed, by recognizing a closer involvement of the private sector in the implementation of the law without questioning the final responsibility of government; fourth, the EU and the Member States should focus their interventions on essential components of privacy and data protection, for pragmatic reasons and for jurisdictional reasons; fifth, the EU and the Member States could reconsider the main principles of data protection, in order to adapt these principles to the changed circumstances, however without giving up on the need for protection of individuals. This fifth direction is for the long term, if only because the main principles of data protection are laid down in EU primary law.

The contribution of the EU legislator plays a key role in regaining control. A regulation is the appropriate legislative instrument, also for the public sector.

Data protection as a right to fair processing requires that the legislator gives effect to the core elements of data protection, mentioned in the Charter. The focus in the General Data Protection Regulation (GDPR) is the adaptation of legislative arrangements to the new circumstances. One thing the GDPR explicitly omits, is addressing the principles or values of privacy and data protection as such.

This study recommends developing a strategy for the legislator on how to regain control, based on the five directions mentioned above and focusing on the impact of the internet on the main principles of data protection. On the long term, this strategy could result in the re-thinking of the principles or values of privacy and data protection.
An essential part of the enforcement of EU data protection law is assigned to expert bodies, which are primarily the independent data protection authorities (DPAs) of the Member States. These DPAs are independent public authorities with a variety of roles: ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers\textsuperscript{2705}. In short, not only the mandate of the EU under Article 16 TFEU is broad, but so is the mandate of the DPAs within the EU and the Member States.

The embedding of the role of DPAs in primary law gives them constitutional status under EU law. This study qualifies the DPAs as a new branch of government, in the theory of Vibert.\textsuperscript{2706} DPAs do not derive their power from the other branches of government, as agents vis-à-vis a principal. By contrast, they are competent to supervise these other branches of government, the traditional trias politica. This new branch of government could be instrumental in restoring trust, if the authorities are completely independent and operate within a context of checks and balances. The DPAs should act within the limits of their competence in accordance with requirements of independence, effectiveness and accountability. Similar requirements are developed for good governance of agencies.

This study proposes that a model for good governance for data protection authorities be developed. This model is inspired by the LITER Good Agency Principles\textsuperscript{2707}, aiming at making agencies work better.

This study presents three models of cooperation of DPAs: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models compose a layered structure for an independent, effective and accountable control on EU data protection.

At present, the control on the compliance of data protection rules is not centralized at the EU level. Although considerations of effectiveness plead in favour of a uniform and harmonized approach of the control, this does not mean that centralization of the control would be the preferred option, at least not in the immediate future. Centralization of the control is also not favoured in any of the contributions of the EU institutions in the legislative process in the GDPR.

The study recommends elaborating the layered structure, as structure for a better governance of control on data privacy and data protection in the EU. This layered structure is not meant to centralize essential parts of the decision making by DPAs to the European level, but to ensure that where the European level is involved in the control on data protection rules, appropriate standards are in place.

\textsuperscript{2707} A. Ottow, Market & Competition Authorities, Good Agency Principles, Oxford 2015, mainly Chapter 3.
The EU as an actor in the external domain should take responsibility for globalization, based on the claim that EU values have a normative strength and are universally applicable. The EU has global power through the legal standards representing these values.

In order to ensure effective protection of individuals on the internet, the preferred strategy should be the unilateral strategy, aiming at exporting EU values in the international domain. The EU could thereby use facilities offered by the Council of Europe, such as the possibility that non-European countries adhere to Convention 108. As part of this strategy on practical level, bridges should be built with likeminded countries.

In addition, the bilateral strategy should be explored, focusing on mutual recognition, standardisation processes or enforcement cooperation, based on the communalities between the systems, but also accepting the differences. The OECD could possibly play a role.

In the long term, a UN-Treaty would ensure best protection (the multilateral approach). The EU should take initiatives in order to facilitate the adoption of such a Treaty, with the ambition to achieve a minimum standard of data protection.

Finally

For the short term, the General Data Protection Regulation means a significant step for data protection in the European Union, with relevance for all actors under Article 16 TFEU.

The General Data Protection Regulation does however not solve all weaknesses in the system. It remains to be seen whether, in the long term perspective, the Regulation suffices. Subjects that in any event require further action on the longer term are:

- The adaptation of the substantive principles of data protection.
- The fine-tuning of the role of the Member States under Article 16 TFEU.
- The centralization of the supervision of global internet companies

These subjects should be further explored in academic research in the coming years.
De Europese Unie als een constitutionele waakhond van privacy en gegevensbescherming op internet: het verhaal van artikel 16 VWEU ("The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU")

KORTE SAMENVATTING

Deze studie komt voort uit de perceptie dat overheden controle verliezen over maatschappelijke ontwikkelingen, als gevolg van globalisering en technologische ontwikkelingen. Deze verschijnselen verhinderen een effectieve bescherming van fundamentele waarden in democratische samenlevingen. Voorbeelden van problemen zijn de extensieve toegang van de Amerikaanse NSA tot persoonsgegevens van Europeanen, zoals naar voren kwam in de onthullingen van Edward Snowden, en de moeite die het kost om in een big data omgeving te zorgen dat de grote internetbedrijven goede privacy-voorwaarden hanteren, waarbij de burger nog enige controle heeft over wat er met zijn gegevens gebeurt.

Privacy en gegevensbescherming zijn fundamentele waarden in de democratische rechtsstaat. The EU Verdragen hebben de Europese Unie een breed geformuleerde opdracht gegeven om deze grondrechten effectief te beschermen, door middel van rechterlijk toezicht, wetgeving en toezicht door onafhankelijke autoriteiten. Het mandaat is nu op constitutioneel niveau vastgelegd en geeft de Unie het vermogen om op te treden als een constitutionele waakhond van privacy en gegevensbescherming.

Meer precies, Artikel 16 van het EU Werkingsverdrag (VWEU), gelezen in samenhang met de artikelen 7 en 8 van het Grondrechtenhandvest, legt de taken vast van de Unie op dit terrein. Artikel 16 (1) VWEU en de artikelen 7 en 8 Handvest specificeren het recht dat de Unie moet garanderen, uiteindelijk onder toezicht van het Europees Hof van Justitie, artikel 16 (2) VWEU geeft de wetgever de opdracht regels te stellen en tot slot moet het toezicht door de onafhankelijke autoriteiten worden gegarandeerd, een vereiste van artikel 16 (2) VWEU en artikel 8 (3) Handvest.

Artikel 16 VWEU geeft de Unie een specifiek mandaat om bescherming te verzekeren, in aanvulling op de algemene verplichting voor de Unie - en voor de nationale overheden wanneer zij handelen binnen de reikwijdte van het Europees recht - om de rechten in het Handvest te respecteren. Artikel 6 VWEU bepaalt dat de Unie moet optreden ter bescherming van de grondrechten van privacy en gegevensbescherming.
De opdracht van artikel 16 VWEU is breed geformuleerd en geeft de Unie - in beginsel - handelingsvermogen en het vermogen om het verschil te maken. Dit is een onderwerp waar de Unie succesvol kan zijn, door een wereldwijd en technologisch ingewikkeld probleem aan te pakken.

Deze specifieke opdracht van de Unie is het onderwerp van deze studie. De studie analyseert de bijdragen van specifieke actoren binnen het Europese rechtsbestel. Dit zijn de rechterlijke macht, de EU wetgever, de onafhankelijke toezichthouders, de samenwerkingsmechanismen van deze toezichthouders en, tot slot, de Unie als zodanig in de internationale arena. De legitimiteit en de effectiviteit van de Unie en van het handelen van de verschillende actoren zijn de invalshoeken voor de analyse.

**Algemene conclusies**

De analyse laat zien dat een succesvol gebruik van de bevoegdheden van de Unie op basis van artikel 16 VWEU mogelijk is, in overeenstemming met vereisten van legitimiteit en de effectiviteit. De analyse laat ook zien dat een ambitieuze aanpak nodig is, gelet op de grote uitdagingen van de informatiemaatschappij.

Het succes van de Unie in de uitvoering van haar opdracht is essentieel voor personen wier grondrechten op het spel staan. Het is ook essentieel voor onze democratische rechtsstaten. Daar komt bij dat als de Unie haar ambities kan waarmaken en een effectieve bijdrage kan leveren aan de bescherming van privacy en gegevensbescherming op internet, dit resultaat legitimiteit geeft aan het mandaat van de Unie en - in een wijder perspectief - het vertrouwen in de Unie, dat thans onder druk staat, kan vergroten. Indirect kan dit ook bijdragen aan het vertrouwen in nationale overheden.

Deze studie is optimistisch. De Unie heeft een geschikt mandaat op dit terrein, met - in beginsel - onbeperkte taken voor de rechterlijke macht, de wetgever en de onafhankelijke toezichthouders. Het mandaat maakt ook een succesvolle samenwerking van de toezichthouders mogelijk en stelt de Unie in staat om internationaal effectief te opereren.

Dit optimisme is tevens gebaseerd op de sterke positie van Europa in het internationale domein, gebaseerd op wat wel het Brussels effect wordt genoemd. Het recht kan het verschil maken in de informatiemaatschappij op voorwaarde dat de beschikbare instrumenten op een intelligente manier worden gebruikt.

Het succes van de Unie in de uitvoering van het mandaat voortvloeiend uit artikel 16 VWEU hangt af van de wijze waarop de Unie vereisten van legitimiteit en effectiviteit weet te verzoenen. Een succesvolle uitvoering van het mandaat laat zien dat de Unie in staat is bescherming te bieden op het wereldwijde internet. Kortom, dit is een terrein waar niet alleen het recht, maar ook de Europese Unie het verschil kan maken.

---

Deze studie stelt dat artikel 16 VWEU erbij gebaat is de begrippen privacy en gegevensbescherming toe te passen met inachtneming van de gewijzigde omstandigheden op internet. Ook de verhouding met andere grondrechten, zoals de vrijheid is veranderd door het internet.

In een internet omgeving heeft het niet langer zin privacy en gegevensbescherming als twee te onderscheiden grondrechten te beschouwen. Immers, iedere verwerking van persoonsgegevens kan potentiëel de privacy van de burger aan te tasten, in het bijzonder als gevolg van big data. Kortom, deze twee rechten, die in het EU Grondrechtenhandvest worden onderscheiden, maken deel uit van één systeem. Bovendien is op internet gegevensbescherming geen recht die verwerking onmogelijk maakt - het is geen verbodsrecht - maar wel een recht van iedere burger dat zijn of haar gegevens eerlijk worden verwerkt.

Op internet botsen privacy en gegevensbescherming steeds vaker met informatiegrondrechten, dit terwijl de bescherming van eerstgenoemde rechten steeds moeilijker wordt.

Het EU Hof van Justitie houdt in zijn rechtspraak rekening met de noodzaak compensatie te bieden voor het - gepercipieerde - verlies van controle op persoonsgegevens. Het doet dit op basis van de huidige EU wetgeving en in het bijzonder Richtlijn 95/46. De EU wetgever zal spoedig een nieuw wettelijk kader voor gegevensbescherming aanwenden, dat wezenlijke vernieuwingen met zich meebrengt en de bescherming naar een hoger plan moet tillen. De EU verdragen erkennen de wezenlijke rol van de toezichthouders die een hoge mate van onafhankelijkheid genieten, zoals ook het Hof heeft bevestigd. De toezichthouders en hun samenwerkingsstructuren spelen een belangrijke rol in de ontwikkeling van de Europese gegevensbescherming. Die rol wordt verder versterkt door het nieuwe wettelijk kader. Tot slot, de Unie speelt een actieve rol in de internationale arena, ook via de bijdragen van de verschillende actoren.

Specifieke bevindingen, gerelateerd aan de verschillende actoren en rollen

Artikel 16 VWEU verschaft de Unie een stevig mandaat en verzekert dat privacy en gegevensbescherming per definitie binnen de reikwijdte van het EU recht vallen. De hoge ambities van de Unie zouden compensatie moeten bieden voor het verlies van controle op internet. Echter, de Unie is niet de enige waakhond op internet. Ook de lidstaten moeten een rol spelen. Het Europees stelsel van executief federalisme mag echter niet het beschermingsniveau aantasten.

Een goede uitvoering van het EU mandaat draagt bij aan de sociale legitimatie van de Unie en kan ook een element zijn dat vormt geeft aan het Europees burgerschap. De EU rol moet ook legitiem zijn ten opzichte van de lidstaten. Een effectieve uitvoering geeft de Unie wat output-legitimiteit wordt genoemd. De Unie moet niet alleen de beginselen van privacy formuleren, maar ook zorgdragen voor een effectieve praktijk. Dit vergt een doelmatige

---

instrumentkeuze, die niet alleen de rollen van de verschillende publieke actoren versterkt, maar ook private partijen betrekt bij de uitvoering, waarbij de eindregie overigens wel bij de overheid moet blijven.

Deze studie bevat en aantal suggesties om de verschillende publieke en private te betrekken in het managen van gegevensbescherming. De studie stelt voor om op basis van deze suggesties een strategie te ontwikkelen, waarin ook de verantwoordelijkheden van de verschillende partijen nadrukkelijk worden onderscheiden.

In de laatste jaren heeft het Hof van Justitie een belangrijke voortrekkersrol gespeeld, rekening houdend met de impact van de informatiesamenleving. Duidelijke voorbeelden zijn twee arresten uit 2014, Google Spain over de verwijdering van zoekgegevens, en Digital Rights Ireland, waarbij de richtlijn over het bewaren van communicatiegegevens werd vernietigd. Ook het recente Schrems arrest draagt aan dit beeld bij.

Tegen deze achtergrond stelt de studie een eenvoudige taxonomie van grondrechten voor, die het mogelijk maakt een differentiatie te maken in beschermingsniveau, gebaseerd op het belang van een bepaald grondrecht voor de democratische rechtsstaat. Deze taxonomie ziet er als volgt uit:

a. Absolute grondrechten waar geen beperking op mogelijk is. Dit zijn de rechten in titel I Handvest, waardigheid.

b. Rechten met een grote impact op de menselijke waardigheid en de democratie, maar zonder absoluut karakter (zoals privacy en gegevensbescherming).

c. Sociale, culturele en economische rechten. Verder categorieën zijn de beginselen uit het Handvest (genoemd in artikel 51(2) en 52 (5), de fundamentele vrijheden uit de EU Verdragen en verdere algemene belangen.

De studie onderscheidt vijf oplossingsrichtingen voor de EU wetgever om controle te herwinnen. Ten eerste, de bestaande wettelijke instrumenten kunnen worden uitgelegd op een wijze die rekening houdt met de gewijzigde omstandigheden. Ten tweede, de wettelijke arrangementen worden aangepast aan de nieuwe omstandigheden. Ten derde, de gewijzigde verhouding tussen de publieke en de private sector wordt geadresseerd, door de private sector sterker te betrekken bij de implementatie, overigens zonder afbreuk aan de eindregie van de overheid. Ten vierde, de EU en de lidstaten worden gestimuleerd om hun interventies te focussen op wezenlijke elementen van bescherming, om pragmatische redenen en om redenen van internationale rechtsmacht. Ten vijfde, de wetgever stelt de belangrijkste beginselen van gegevensbescherming ter discussie, teneinde de beginselen aan te passen aan de praktijk, maar zonder de behoefte aan bescherming op te geven. Deze vijfde oplossingsrichting is voor de lange termijn, ook al omdat wezenlijke beginselen op verdragsniveau vastliggen.

De bijdrage van de wetgever is essentieel, om controle te herwinnen. Een verordening is het juiste instrument, ook voor de publieke sector. Gegevensbescherming als een recht op eerlijke
verwerking vereist dat de wetgever uitvoering geeft aan de belangrijkste beginselen van bescherming, die in het Handvest zijn opgenomen. De nieuwe verordening past de wettelijke arrangementen aan de nieuwe omstandigheden aan. De verordening laat één ding nadrukkelijk na: de aanpassing van de beginselen.

Deze studie stelt voor dat de EU wetgever een strategie ontwikkelt, gebaseerd op de vijf genoemde oplossingsrichtingen en gericht op de consequentie van internet. Op lange termijn moet zo’n strategie kunnen leiden tot een heroverweging van inhoudelijke beginselen van privacy en gegevensbescherming.

Een essentieel deel van het toezicht is opgedragen aan expert-organen (“expert bodies”), in het bijzonder de onafhankelijke toezichthouders die vooral bekend staan onder het Engelstalige acronym “DPAs”. De DPAs zijn onafhankelijke publieke organen – vooral van de lidstaten – met een reeks aan rollen: ombudsman, auditeur, consultant, opleider, beleidsadviseur, onderhandelaar en handhaver. Het mandaat van de DPAs is dus ruim.

De inbedding van de rol van de DPAs in het primaire Europees recht geeft deze organen een constitutionele status in het Europees recht. De studie kwalificeert deze organen als een nieuwe overheidsmacht, gebaseerd op een theorie van Vibert.2710 DPAs ontlenen hun bevoegdheid niet aan de andere overheidsmachten, als agenten ten opzichte van een principaal. In tegendeel, de DPAs zijn zelfs bevoegd toezicht te houden op de andere overheidsmachten, de traditionele trias politica. Deze nieuwe overheidsmacht kan instrumenteel zijn voor het herstellen van vertrouwen, gesteld dat de DPAs opereren in volledige onafhankelijkheid, maar ook binnen een stelsel van checks en balances. DPAs moeten handelen binnen de grenzen van hun bevoegdheid, in overeenstemming met eisen van onafhankelijkheid, effectiviteit en verantwoordelijkheid. Dergelijke eisen gelden ook voor agentschappen, waarvan de DPAs overigens wel moeten worden onderscheiden.

Deze studie stelt voor een model te ontwikkelen voor goed bestuur door de DPAs en geeft de uitgangspunten voor het model, geïnspireerd op de zogenoemde LITER beginselen voor agentschappen, zoals beschreven door Ottow.2711

De studie presenteert ook drie modellen voor de samenwerking van DPAs, te weten: horizontale samenwerking, een gestuctureerd netwerk en samenwerking in een Europese DPA. Deze drie modellen vormen een gelaagde structuur voor onafhankelijk, effectief en verantwoordelijk toezicht.

Thans is het toezicht op de naleving van de regels voor gegevensbescherming niet gecentraliseerd op Europees niveau. Hoewel overwegingen van effectiviteit zouden pleiten voor een uniforme en geëntegereerde aanpak van het toezicht, stelt deze studie geen centralisatie voor, althans niet voor de komende jaren. Geen enkele instelling of adviseur

pleitte overigens voor centralisatie tijdens de onderhandelingen over de Verordening gegevensbescherming.

De studie pleit wel voor een betere organisatie van het toezicht op privacy en gegevensbescherming in de EU, via de gelaagde structuur. Deze gelaagde structuur heeft niet tot doel delen van het toezicht te centraliseren, maar wel om te verzekeren dat waar het Europees niveau is betrokken, behoorlijke procedures gelden.

**De EU als een actor in de internationale arena** moet verantwoordelijkheid nemen voor globalisering, gebaseerd op de claim dat EU waarden een normatieve waarde hebben en universeel toepasbaar zijn. De EU heeft een wereldwijd gezag dankzij de wettelijke standaarden die deze waarden vertegenwoordigen.

Teneinde effectief bescherming te kunnen bieden op het internet, heeft deze studie de voorkeur voor een unilaterale strategie, met als doel het exporteren van de Europese waarden in het internationale domein. De EU kan daarbij gebruik maken van de faciliteiten die de Raad van Europa biedt, zoals de mogelijkheid dat niet-Europese landen toetreden tot Conventie 108 van de Raad. Als onderdeel van deze unilaterale strategie zouden wel op praktisch niveau bruggen worden geconstrueerd met derde landen die vergelijkbare opvattingen hebben over privacy, zoals de Verenigde Staten.

Daarenboven zou een bilaterale strategie moeten worden geëxploreerd, die is gericht op wederzijdse erkenning, standaardisatie of samenwerking in de handhaving. Deze strategie kan gebaseerd zijn op gemeenschappelijke opvattingen, maar moet ook verschillen accepteren. De OESO zou hierbij een rol kunnen spelen.

Op lange termijn zou een VN-Verdrag de beste bescherming kunnen bieden (de multilaterale benadering). De EU zou initiatieven moeten nemen om het aannemen van zo’n verdrag te bevorderen, met de ambitie om wereldwijd een minimum niveau van gegevensbescherming overeen te komen.

**Tot slot**

Voor de korte termijn vormt de Algemene Verordening Gegevensbescherming een wezenlijke stap voorwaarts, met relevantie voor alle actoren op basis van artikel 16 VWEU.

De verordening lost echter niet alle zwaktes in het systeem op. Het bevalt te bezien of voor de langere termijn de verordening volstaat. Onderwerpen die in elke geval verdere actie vragen voor de langere termijn zijn:

- a. De aanpassing van de inhoudelijke beginselen van gegevensbescherming.
- b. De fine tuning van de rol van de lidstaten op basis van artikel 16 VWEU.
- c. De centralisatie van het toezicht op wereldwijd opererende internet bedrijven.

Deze onderwerpen lenen zich voor academisch onderzoek in de komende jaren.
Annex I: Consulted documents

Legislation and proposed legislation

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195/3.


Commission Decision, C(2008) 927 final, declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/ DoubleClick).


Council Decision on the strengthening of Eurojust and amending Decision 2002/187/JHA


European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)).


Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012), 10 final.
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012), 11 final.


Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.


Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180/1.


Various Council documents on Council Public Register, re Interinstitutional file 2012/0011 (COD), e.g. 18031/13 (19 Dec 2013, full version on lobbyplag.eu), 14788/1/14 (13-11-2014), - Preparation of a general approach, Note from Presidency to Council, 11 June 2015, 9565/15.

Case law

Court of Justice of the European Union


Case C/64, Costa v. E.N.E.L., ECLI:EU:C:1964:66.

Case 22/70, Commission v. Council (known as AETR or ERTA).

Case 33/76, Rewe-Zentraleinanzi, ECLI:EU:C:1976:188.

Case 44/79, Hauer, EU:C:1979:290, on fundamental rights and the unity of the Common Market and on the right to property.

Case 98/80, Romano, EU:C:1981:104, on legislative powers in the EU.

Case 13/83, Parliament v Council, EU:C:1985:220, on failure to act by Council (transport).


Case C-260/89, ERT, [vindplaats], on the fact that exceptions to the freedoms should be compatible with the fundamental rights.

Case C-54/96, Dorsch Consult Ingenieursgesellschaft, ECLI:EU:C:1997:413, on independence.

Case C-285/98, Kreil, ECLI:EU:C:2000:2, on internal and external security.

Case C-269/90, Technische Universität München, ECLI:EU:C:1991:438, at 13-14, on the duty of care and right to a hearing.

Case C-184/99, Grzeczyk, ECLI:EU:C:2001:458, in EU citizenship.

Case C-11/00, Commission v European Central Bank, ECLI:EU:C:2003:395.

Case C-50/00P, Unión de Pequeños Agricultores v Council of the European Union, ECLI:EU:C:2002:462.

Case C-112/00, Schmidberger, ECLI:EU:C:2003:333.

C-340/00 P - Commission v Cwik, ECLI:EU:C:2001:701, on the freedom of expression.

Case C-101/01, Lindqvist, ECLI:EU:C:2003:596, on the publication of personal data on the internet.

Case C-465/00, Österreichischer Rundfunk and others, ECLI:EU:C:2003:294, on privacy and data protection, in context ECHR.

Case C-36/02, Omega Spielhallen, [vindplaats]

Opinion 1/2003 (Lugano Convention).

Case C-53/03, Syfait and Others, ECLI:EU:C:2005:333, on independence.

Case C-503/03, Commission v Spain, ECLI:EU:C:2006:74, on composite decision making procedure and SIS.

Joined cases C-317/04 and C-318/04, European Parliament v Council Union (C-317/04) and Commission (C-318/04), ECLI:EU:C:2006:346, on Passenger Name Records of air passengers.


Case C-387/05, Commission v Italy, ECLI:EU:C:2009:781, on exception of public security.
Joined cases C-402/05P and 415/05P, Kadi and Al Barakaat, EU:C:2008:461, on the protection of fundamental rights, also in international (UN) context.

Case C-275/06, Promusicae, EU:C:2008:54.

Case C-301/06, Ireland v Parliament and Council, EU:C:2009:68, on data retention.

Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (Satamedia), EU:C:2008:727.

Opinion AG Poiares Maduro in Case C-127/07, Arcelor, on national identity.

Case C-424/07, Commission v Germany, EU:C:2009:749, on independence of telecommunications regulators.

Case C-518/07, Commission v Germany, EU:C:2010:125, on the independence of data protection authorities.


Case C-555/07, Küçükdeveci, EU:C:2010:21.


Case C-585/08, Panmer and Hotel Alpenhof, EU:C:2010:740, on directing activities to a jurisdiction.

Case C-34/09, Ruiz Zambrano, [vindplaats].

Opinion AG Sharpston, [vindplaats].

Joined cases C-92/09 and C-93/09, Schecke (C-92/09) and Eifert (C-93/09) v Land Hessen, EU:C:2010:662, on Articles 7 and 8 of the Charter.


Case C-145/09, Tsakouridis, EU:C:2010:708, on imperative grounds of public security.

Case C-208/09, Sayn-Wittgenstein, EU:C:2010:806, on national identity.


Case C-279/09, DEB Deutsche Energiehandels- und Beratungsgesellschaft, EU:C:2010:811, on Article 47 Charter.

Case C-324/09, L’Oréal and Others, EU:C:2011:474, e.g. on internet monitoring.

Case C-348/09, P.I., EU:C:2012:300, on imperative grounds of public security.


Case C-543/09, Air Transport Association of America and Others, EU:C:2011:771.

Joined cases C-411/10 and C-493/10, N.S., and M.E. and Others, EU:C:2011:865, on Member States and fundamental rights.


Case C-461/10, Bonnier Audio, EU:C:2012:219.

Case C-614/10, Commission v Austria, EU:C:2012:63.


Case C-617/10, Åkerberg Fransson, EU:C:2013:280, on Article 51 of the Charter.


Case C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777.

 Joined cases C-584/10 P, C-593/10 P and C-595/10 P, Commission and others v Kadi (Kadi II), EU:C:2013:518.


Case C-199/11, Otis and Others, EU:C:2012:684, on the Charter as yardstick.

Case C-277/11, M.M., EU:C:2012:744, on the scope of Article 41 of the Charter.

Case C-283/11, Sky Österreich, EU:C:2013:28, on Articles 17 and 16 Charter.

Opinion AG Bot, [vindplaats]

Case C-300/11, ZZ, EU:C:2013:363, on effective judicial protection and on state security.


Case C-399/11, Melloni, EU:C:2013:107, on the Charter and the EAW.


Case C-93/12, Agroksulting-04, EU:C:2013:432, on ‘proximity’.

Case C-131/12, Google Spain and Google Inc, EU:C:2014:317.

Case C-176/12, Association de médiation sociale, EU:C:2014:2, on horizontal effect Charter.

Joined Cases C-199 to C-201/12, Minister voor Immigratie en Asiel v X (C-199/12) and Y (C-200/12) and Z v Minister voor Immigratie en Asiel (C-201/12), Minister voor Immigratie en Asiel v X (C-199/12) and Y (C-200/12) and Z v Minister voor Immigratie en Asiel (C-201/12), [vindplaats]


Case C-270/12, UK v EP/Council, [vindplaats], on ESMA
Opinion AG Jääskinen, [vindplaats]

Case C-288/12, Commission v Hungary, EU:C:2014:237, on the independence of data protection authorities.

Case C-291/12, Schwarz, EU:C:2013:670.

Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, on Articles 7 and 8 of the Charter.
Case C-314/12, UPC Telekabel Wien, EU:C:2014:192, copyright, conducting business, intermediaries and balancing fr’s

Case C-390/12, Pfleger, EU:C:2014:281, on Articles 15-17 Charter
Opinion AG Sharpston, [vindplaats], on e.g. scope EU law.

Case C-473/12, IPI, EU:C:2013:715, on exceptions of Art 13 of 95/46.


Case C-580/13, Coty Germany, ECLI:EU:C:2015:485, on balancing fr’s

Case C-615/13P, ClientEarth and PAN Europe v EFSA, EU:C:2015:489.

Case C-62/14, Gauweiler and others, EU:C:2015:400.

Case C-129/14PPU, Spasic, EU:C:2014:1918, ne bis in idem in Schengen and Charter.

Case C-157/14, Neptune Distribution, ECLI:EU:C:2015:460 (pending).

Case C-201/14, Bara, ECLI:EU:C:2015:638.

Case C-230/14, Weltimmo, ECLI:EU:C:2015:639.

Case C-362/14, Schrems, (pending)

Case C-582/14, Breyer (pending).

Opinion 1/15 on Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (pending).

Case C-192/15, Rease and Wullems (pending).

Case C-398/15, Manni (pending), follow up on Google Spain.

General Court/Court of First Instance


Case T-79/12, Cisco and Mesagenet, [vindplaats]


European Court of Human Rights
Klass and Others v Germany, 6 September 1978, §§ 49-50, Series A No. 28.

Leander v Sweden, 26 March 1987, Application No. 9248/81


Niemietz v Germany, ECHR (1992) A-251-B.

Rotaru v Romania, No. 28341/95, ECHR 2000-V, on secret surveillance.

Weber and Saravia v Germany (dec.), No. 54934/00, § 94, ECHR 2006-XI.

Liberty and Others v the United Kingdom, No. 58243/00, § 62, 1 July 2008.

Bankovic v Belgium, Application 52207/99, on jurisdictional issues.

Assanidze v Georgia, Application No. 71503/01, 8 April 2004, on the separation of powers.


Axel Springer v Germany, Application No. 39954/08.

I. v Finland, Application No. 20511/03, 17 July 2008, on medical data.

Nada v Switzerland, Application No. 10593/08, 12 September 2012, on post 9/11 measures.

Brunet v France, Requête No 21010/10, 18 septembre 2014 **

Delfi AS v Estonia, Application No. 64569/09, 16 June 2015

Permanent Court of International Justice


US Supreme Court

389 U.S. 347 (1967), Katz v United States, on eavesdropping public telephone booth and 4th amendment.

442 U.S. 735 (1979), Smith v Maryland, on metadata.

110 S. Ct. 1056 (1990), United States v Verdugo-Urquidez, on extraterritoriality.


132 S. Ct. 945 (2012), United States v Jones, on the police having attached a GPS device to the undercarriage of Jones’ car.


Electronic Privacy Information Center (EPIC) Amicus Brief.
[case number], Los Angeles v Patel et al., no. 13-1175, 22 June 2015.

*Other national Courts*

Bundesverfassungsgericht Germany, Case 1 BvR 357/05, Judgment of 15 February 2006, on the German ‘Aviation Security Act’.

Bundesverfassungsgericht Germany, Joined cases 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Judgment of 2 March 2010, on data retention. Press release No. 11/2010 of 2 March 2010.


Bundesverfassungsgericht Germany, Case 2 BvR 2661/06, Judgment 6 July 2010, Honeywell.


US Court of Appeals, for the Second Circuit, ACLU v Clapper, [vindplaats].

*Policy documents*


Article 29 Data Protection Working Party, Advice paper of 20 April 2011 on the practical implementation of the Article 28(6) of the Directive 95/46/EC.


Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González”, WP 225.


Article 29 Working Party, Letter to Google on the right to be delisted, 6 January 2015.

Big Data and Privacy: A Technological Perspective. Executive Office of the President, President’s Council of Advisors on Science and Technology, (“PCAST report”) May 2014.
http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (“Podesta report”), May 2014.
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

Centre for Information Policy Leadership, The Role of Risk Management in Data Protection,

Centre for Information Policy Leadership, Various documents on accountability,


Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things : an action plan for Europe, COM/2009/0278 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245 final.


Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet Policy and Governance Europe's role in shaping the future of Internet Governance, COM/2014/072 final.


Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A renewed EU strategy 2011-14 for Corporate Social Responsibility, COM(2011) 681 final.


Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation for better results - An EU agenda, COM(2015) 215 final


European Data Protection Supervisor, Opinion on the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, OJ (2009), C 276/1.

European Data Protection Supervisor, Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ C 147/1.


European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package.


European Data Protection Supervisor, Opinion of 26 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe".


European Data Protection Supervisor, Letter of 13 November 2013 to Mr Juan Fernando López Aguilar, Chair of the LIBE-Committee of the European Parliament concerning the data protection supervision on Europol.


European Data Protection Supervisor, Preliminary Opinion of 26 March 2014 on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”.

European Data Protection Supervisor, Opinion of 4 June 2014 on the future development of the area of freedom, security and justice.


European Parliament resolution of 15 January 2013 with recommendations to the Commission on a Law of Administrative Procedure of the European Union (2012/2024(INL)).

European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance

European Parliament resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (2014/2966(RSP)).


Joint statement issued following a meeting of the ministers of the interior in Paris, 11 January 2015 (following Charlie Hebdo).


The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 February 2015, [https://drive.google.com/file/d/0B1UgZshetMd4cEI3SJhV0hNbDA/view](https://drive.google.com/file/d/0B1UgZshetMd4cEI3SJhV0hNbDA/view).


UN General Assembly plenary on 18 December, 2014, Resolution “Right to Privacy in the Digital Age” (A/RES/69/166).


Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De publieke kern van het internet, Naar een buitenlands internetbeleid, Amsterdam 2015.


**Other references**


Alsenoy, Brendan van a.o., 201, From social media service to advertising network, A critical analysis of Facebooks Revides Polucies and Terms.


Blockmans, Steven and Ramses A. Wessel (eds), 2012, Principles and practices of EU external Representation, Cleer Working Papers 2012/5.


Carrera, Sergio, Gloria González Fuster, Elspeth Guild, Valsamis Mitsilegas, 2015, “Access to Electronic Data by Third-Country Law Enforcement Authorities, Challenges to EU Rule of Law and Fundamental Rights”, CEPS.


Court of Justice of the European Union, The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law - La Cour de Justice et la Construction de l'Europe: Analyses et Perspectives de Soixante Ans de Jurisprudence, Published on the unique occasion of its 60th anniversary.


Eeten, Michel JG van, and Milton Mueller, 2013, “Where is the governance in Internet governance?”, New Media & Society August 2013 vol. 15 no. 5 720-736.


Volume 1, The Protection of Fundamental Rights Post-Lisbon: The Interaction between the Charter of the
Fundamental Rights of the European Union, the European Convention on Human Rights and National
Constitutions,
Volume 3: The Area of Freedom, Security and Justice, Including Information Society Issues,
Tartu University Press.

FIDE Congress, 2014, Reports of the FIDE Congress in Copenhagen,
Volume 1, Constitutional and Institutional Aspects of the Economic Governance within the EU,
DJOF Publishing.


Gloria Gonzalez Fuster and Serge Gutwirth, Ethics, law and privacy: Disentangling law from ethics in privacy discourse, 2014, eceexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6893376


Gloria González Fuster, Curtailing a right in flux restrictions of the right to personal data protection, in: “Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime, Artemi Rallo Lombarte, Rosario García Mahamut (eds).


Greenwald, Glenn, No Place to Hide: Edward Snowden, the NSA and the Surveillance State.


Grotius, Hugo, The Freedom of the Sea, Or, The Right Which Belongs to the Dutch to Take Part in the East Indian Trade, available at:


Kuner, Christopher, 2013, Transborder Data Flows and Data Privacy Law.

Kuner, Christopher et al., 2015, “Internet Balkanization gathers pace: is privacy the real driver?”, International Data Privacy Law, 2015, Vol. 5, No. 1.


Lenaerts, Koen and Jose A. Gutiérrez-Fons, “The constitutional allocation of powers and general principles of EU law”, [tijdschrift], Issue 6, 1629–1669.


Middelaar, Luuk van, The Passage to Europe: How a Continent Became a Union.


Pérez Asinari, María Verónica and Pablo Palazzi (eds.), 2008, Défis du droit a la protection des données, Perspectives du Droit Européen et Nord-Américain – Challenges of privacy and data protection law, Perspectives of European and North-American Law, Cahiers du Centre de Recherches Informatique et Droit.


Prechal, Sacha, “The Court of Justice and effective judicial protection: what has the Charter changed?”, in: Protecting fundamental rights in the international arena: public, private and European law perspectives
Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions, Amsterdam / Cambridge, September 2015.


Reidenberg, Joel R. a.o., 2013, Internet Jurisdiction, Survey of Legal Scholarship Published in English and United States Case Law, Fordham Center on Law and Information Policy.


Rotenberg, Marc, Julia Horwitz and Jeramie Scott (eds), Privacy in the Modern Age, The Search for Solutions.


Ryngaert, Cedric, 2007, Jurisdiction in International Law, United States and European Perspectives, KU Leuven: Doctorate Thesis.


Schneier, Bruce, 2015, Data and Goliath.


Svantesson, Dan Jerker B., 2013, Extraterritorial Data Privacy Law.

Tamanaha, Brian, 2007, A Concise Guide to the Rule of Law, St. John’s University School of Law.


VANAF HIER NOG OP AUTEUR EN ALFABETISCH (TUSSEN DE WERKEN HIERBOVEN ONDER 4)


Mireille Hildebrandt, Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schnitt, Grotius in cyberspace, University of Toronto Law Journal, Volume 63, Number 2, Spring 2013, pp. 196-224.


Hielke Hijmans, Right to have links removed: Evidence of effective data protection, Maastricht Journal of European and Comparative Law, 2014(3).

Christopher Kuner, Google Spain in the EU and international context, Maastricht Journal of European and Comparative Law, 2015(1), at 158-164.

Paul de Hert and Vagelis Papakonstantinou, Google Spain: Addressing Critiques and Misunderstandings One Year Later, Maastricht Journal of European and Comparative Law, 2015, “”.

Herke Kranenborg, Google and the right to be forgotten, EDPL 2015, Issue 1.


Orla Lynskey, The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland’, CMLR 2014, Issue 6, pp. 1789–1811.


H. Hijmans, De ongeldigverklaring van de dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof, NTER September 2014, no 7, p. 245-252 (in Dutch).


Marie-Pierre Granger, Kristina Irion, The Court of Justice and the Data Retention Directive In Digital Rights Ireland - Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection
Andrew Roberts, Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications (pages 535–548), The Modern Law Review, Volume 78, Issue 3


Svantesson, Dan Jerker B., “A layered approach” to the extraterritoriality of data privacy laws.


PRISMS project, sponsored by the EU under the 7th Framework Programme, http://prismsproject.eu/.


Christopher Docksey, Articles 7 and 8 of the EU Charter: two distinct fundamental rights, in **


Jan Philipp Albrecht, No EU Data Protection Standard Below the Level of 1995, EDPL 2015, 1, p.3-4.


P. Oliver, The protection of privacy in the economic sphere before the European Court of Justice, CML Rev October 2009, 1443-1483.


David C. Vladeck, A U.S. Perspective on Narrowing the U.S.-EU Privacy Divide, in “Hacia un Nuevo derecho europeo de protección de datos, Towards a new European Data Protection Regime, Artemi Rallo Lombarte, Rosario García Mahamat (eds).


Jeffrey Rosen, Inside the Stunning Court Smackdown on NSA Spying (journalistic article) http://www.newrepub.com/article/115962/courts-nsa-ruling-against-metadata-collection-fourth-amendment-win

Privacy in Europe: Initial Data on Governance Choices and Corporate Practices


Stefan Kulk, Frederik Zuiderveen Borgesius, Filtering for Copyright Enforcement in Europe after the Sabam cases, European Intellectual Property Review 2012, issue 11, p. 54-58.

Stefan Kulk and Frederik Zuiderveen Borgesius, Freedom of Expression and ‘Right to Be Forgotten’ Cases in the Netherlands After Google Spain, EDPL 2015/2, 113-124.

Christopher Kuner, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges, 2014 **


Monika Kuschewsky (General Editor), Data Protection & Privacy, Jurisdictional Comparisons, Second edition 2014, Thomson Reuters.


Charles D. Raab, Submission to Intelligence and Security Committee of Parliament Privacy and Security Inquiry, 7th February 2014.


Annika Sponselee, Privacy with a View – Part II, Privacy & Practice 01-02/2015, at 71-78.


A. van den Brink, De begrenzing van de bevoegdheden van de Europese Unie als een gedeelde constitutionele opdracht, SEW, Tijdschrift voor Europees en economisch recht, 2014 / 6 (juni).


S.B.M. Princen, The California Effect in the transatlantic relationship, Published by Utrecht, 2002


R. Daniel Kelemen, Suing for Europe, Adversarial Legalism and European Governance, Comparative Political Studies, Volume 39 Number 1, February 2006 101-127.


Martin Shapiro, Comparative Law and Comparative Politics, 53 S. Cal. L. Rev. 537 (1979), Available at: http://scholarship.law.berkeley.edu/facpubs/1170.


Liesbet Hooghe and Gary Marks, Unraveling the Central State, but How? Types of Multi-level Governance, American Political Science Review Vol. 97, No. 2 May 2003.


Special issue: The Constitutional Adulthood of Multi-Level Governance, Maastricht Journal of European and Comparative Law 2014, Volume 21, nr 2


Raya Kardasheva, Trilogues in the EU legislature, King’s College London, Department of European and International Studies, Research Paper, 30 April 2012.


Paul de Hert, Dimitra Stefanatou, The accountability culture in its european union dress. Sticks but no carrots to make the proposed data protection regulation work, in: Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime, Artemi Rallo Lombarte, Rosario García Mahamat (eds).


R. Nazzini, Administrative enforcement, judicial review and fundamental rights in EU competition law: A comparative contextual-functionalist perspective, CML Rev June 2012


Anna-Sara Lind and Jane Reichel, Administrating Data Protection – or the Fort Knox of the European Composite Administration, Critical Quarterly for Administration and Law (EuCritQ), 2014, 1, pp. 44-57.


EU Agencies in between Institutions and Member States, Edited by: Michelle Everson, Cosimo Monda, Ellen Vos, January 2014, ISBN 9041128433


Les agences de l’Union européenne, Sous la Direction de Joël Molinier, Bruylant, en particulier les contributions de

- E. Chiti, Existe-t-il un modele d’agence de l’Union européenne?
- M. Blanquet et N. De Grove-Valdeyron, Le recours à des agences de l’Union en réponse aux questions de sécurité.

E. Chiti, An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies, CML Rev October 2009, pp. 1395-1442.


Miroslava Scholten, THE NEWLY RELEASED ‘COMMON APPROACH’ ON EU AGENCIES: GOING FORWARD OR STANDING STILL?, THE COLUMBIA JOURNAL OF EUROPEAN LAW ONLINE.

- Supervision and supervisory authorities A few introductory remarks, Sacha Prechal, Marleen van Rijswick 1-7
- Regulating regulators through liability, The case for applying normal tort rules to supervisors abstract, Ivo Giesen 8-31
- Independent competition authorities in the EU, Johan W. van de Gronden, Sybe A. de Vries 32-66
- Independent administrative authorities and the standard of judicial review, Saskia Lavrijssen, Maartje de Visser 111-135


Paul De Hert & Gertjan Boulet, Deliverable 2.2 – “Legal reflections for further improving cooperation between data protection authorities”, www.phaedra-project.eu.


Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation, Paolo Balboni, Enrico Pelino, Lucio Scudiero, Computer law & security review 30 (2014) 392-402.
