The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?

Oostveen, M.; Irion, K.

DOI
10.1007/978-3-662-57646-5_2

Publication date
2018

Document Version
Author accepted manuscript

Published in
Personal Data in Competition, Consumer Protection and Intellectual Property Law

UNIVERSITY OF AMSTERDAM

THE GOLDEN AGE OF PERSONAL DATA: HOW TO REGULATE AN ENABLING FUNDAMENTAL RIGHT?

Manon Oostveen

Kristina Irion

Amsterdam Law School Legal Studies Research Paper No. 2016-68

Institute for Information Law Research Paper No. 2016-06

The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?

Manon Oostveen and Kristina Irion

Abstract New technologies, purposes and applications to process individual's personal data are developed on a massive scale. But we have not only entered the 'golden age of personal data' in terms of its exploitation: ours is also the 'golden age of personal data' in terms of regulation of its use. In this contribution, we explain how regulating the processing of an individual's personal data can be a proxy of intervention, which directly or indirectly could benefit other individual rights and freedoms. Understood as an enabling right, the architecture of EU data protection law is capable of protecting against many of the negative short- and long-term effects of contemporary data processing. The new General Data Protection Regulation certainly strengthens aspects of this core architecture but certain regulatory innovations to cope with technological advancements and the data-driven economy appear less capably of yielding broad protection for individuals fundamental rights and freedoms. We conclude that from the perspective of protecting individual fundamental rights and freedoms, it would be worthwhile to explore alternative (legal) approaches of personal data in contemporary data processing.

Keywords privacy, data protection, enabling fundamental rights, big data, General Data Protection Regulation

Table of Contents

Manon Oostveen is PhD Researcher at the Institute for Information Law, University of Amsterdam

M.A.A. Oostveen
Institute for Information Law, University of Amsterdam, The Netherlands
E-Mail: m.a.a.oostveen@ivir.nl

Kristina Irion is Senior Researcher at the Institute for Information Law, University of Amsterdam

K. Irion
Institute for Information Law, University of Amsterdam, The Netherlands
E-Mail: k.irion@ivir.nl

1 Introduction

The protection of personal data is justified against the background of protecting individual's fundamental rights and freedoms, in particular the right to privacy and the new right to the protection of personal data. This chapter articulates the objectives of European Union (EU) data protection law as an enabling human right that renders a discrete contribution to the realisation of a number of other rights and freedoms of the individual. It is argued that EU data protection law's intervention at the stage of processing personal data can produce a number of short- and long-term effects which contribute to preserving individuals' personal autonomy and human dignity.

This research is set against the background of big data applications and algorithmic decision-making, in order to illustrate how both can produce a cascade of effects on individuals' rights and freedoms that goes beyond the core concern of the rights to the protection of private life and personal data. After all, we have entered the 'golden age of personal data' in terms of its exploitation, but also in terms of regulation of its use. EU data protection law's arsenal of regulatory responses to contemporary challenges of personal data processing has just been upgraded with the adoption of the General Data Protection Regulation (GDPR).[1] It is thus timely to assess the capability of the new regulation to mitigate the risks of big data applications and algorithmic decision-making for individual fundamental rights and freedoms.

The argument is developed in three steps. First, the rationale of privacy and data protection as *a)* stand-alone fundamental rights, and *b)* enabling rights, which buttress other fundamental rights and freedoms, is mapped out. As a second step, we turn to the EU legal framework on the protection of personal data, and interrogate its discrete contribution to immediate and long-term interferences with individual's fundamental rights and freedoms. Next, after an introduction to big data applications and algorithmic decision-making we provide an overview of the risks for individual fundamental rights and freedoms. Against this background, the discrete contribution of the GDPR's provisions on automated decision-making and profiling are explained and discussed, followed by the conclusions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1-88.

2 The rationale of fundamental rights protection for privacy and personal data

2.1 Privacy and data protection as stand-alone fundamental rights

In Europe, individuals' privacy and personal data are protected as fundamental rights in the jurisdiction of the Council of Europe and the European Union, respectively. The right to privacy is protected in Article 8 of the European Convention on Human Rights[2] (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union[3] (Charter).[4] The right to privacy broadly protects private and family life as well as individuals' home and correspondence in that it attributes a high level of control to individuals. The right to privacy was interpreted to cover inter alia the protection of personal data against unlawful processing.[5]

The Charter's right to the protection of personal data is a 'third generation' fundamental right, elevating data protection into a self-standing right. The protection of personal data's stand-alone value lies in attributing essential tenets of control to individuals when their personal data is processed by third parties. Under the Charter, an interference with the right to privacy is not a precondition for the applicability of the right to the protection of personal data.[6] Nonetheless, as the private life of individuals is increasingly mediated through the Internet and online services, situations that trigger privacy concerns now often coincide with the processing of personal data and vice versa.[7]

The fundamental rights protecting individuals' privacy and personal data are not ends in themselves. Their protection inherently contributes to furthering other individual fundamental rights and freedoms, which we call privacy's and data protection's *enabling* function.

2.2 Privacy and data protection as enabling rights

European legal literature, while making regular references to personal autonomy and human dignity, has not produced many genuine conceptual contributions on the enabling function of the rights to privacy and to data protection.[8] This may be due to the strong constitutional protections in place and the shift of scholarly attention to judicial interpretations of the fundamental rights and the application of data protection law to a variety of

[2] Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (2007/C 303/02).
[3] Charter of Fundamental Rights of the European Union 2009 (OJ C83/02).
[4] Private life and privacy can be and are used interchangeably. See for more details on the usage and interchangeability of the term González Fuster (2014), particularly p. 81-84 regarding the Convention.
[5] European Court of Human Rights 26 March 1978, case 9248/81, Leander v Sweden, para. 48.
[6] For more on the stand-alone value of privacy and data protection, see for example González Fuster (2014); Lynskey (2014); Tzanou (2013).
[7] Recent examples are for instance EU Court of Justice, Google Spain, C-131/12, ECLI:EU:C:2014:317; EU Court of Justice, Digital Rights Ireland, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
[8] There are notable exceptions, see for example Bernal (2014).

diverse activities involving the processing of personal data. In the social sciences academics are more inclined to interrogate privacy rights as an enabling right, for example in relation to personal autonomy.[9]

Conversely, US legal scholarship continues to argue privacy's important contribution to other individual rights and societal values, resulting in a more profound exploration of the relationship between privacy and other rights and values. Solove rejects the idea that privacy has a unitary value, and instead regards it as a concept that protects a plurality of activities, and is therefore of pluralistic value.[10] In his taxonomy of privacy, Solove touches upon many rights and values that privacy affects, ranging from personal autonomy, freedom of speech to non-discrimination.[11] Richards and Krotoszynski deem privacy indispensable to freedom of speech. Krotoszynski argues that privacy is a precondition for freedom of speech, which makes it also a precondition for democratic self-government.[12] Richards argues the case for intellectual privacy,[13] i.e. the protection of a "*zone to make up our minds freely*", which precedes the actual public expression of ideas and opinions.[14] Roberts takes another angle, by focusing on how privacy facilitates non-discrimination, primarily through obscuring the information necessary to discriminate.[15]

In Europe data protection legislation was often conceived with the enabling function for individuals' fundamental rights and freedoms in mind. Statutory data protection laws explicitly aim at protecting a number of individuals' fundamental rights and freedoms. In Germany, the Federal Data Protection Law adopted in 1976, also the first national statute of its kind in Europe, broadly aims to protect against the impairment of individual interests through protecting personal data in the course of its processing against being abused.[16] The protected individual interests ("*schutzwürdige Belange des Betroffenen*") certainly include personal integrity and private sphere, but also other constitutionally protected individual rights and freedoms, namely freedom of expression, freedom of assembly and association, and freedom of religion.[17] Thus, the formulation of the protected subject-matter has been kept deliberately open for interpretation depending on the circumstances of the processing of personal data.

Similarly, the first French law on the protection of personal data from 1978, refers to human rights, private life, individual or public liberties ("*droits de l'homme, […] vie privée, […] libertés individuelles ou publiques*") as its objective of protection.[18] The French law took much inspiration from the 1975 *Rapport de la Commission*

[9] E.g. Rössler (2005).
[10] Solove (2008), 98–100.
[11] Solove (2006), 513-514 and 529-530.
[12] Krotoszynski (2016), 175.
[13] Richards (2015).
[14] Ibid, 95.
[15] Roberts (2015), 2173.
[16] Article 1 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), 27 January 1977.
[17] Reh (1978), para. 1-6.
[18] Article 1 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. See Dammann / Simitis (1997), 102.

Informatique et Libertés ("*Le Rapport Tricot*") which emphasized the close connection between private life and other individual freedoms.[19]

When adopting the 1995 Data Protection Directive, the EU legislator acknowledged that the directive aims to protect "*fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data*".[20] As Dammann and Simitis observe, this creates a functional link between the protection of personal data to fundamental rights and freedoms in general, instead of narrowing its objective of protection down to the private sphere.[21] They mention the right to freedom of expression, the right to property and the freedom of profession as individual rights and freedoms that data protection law promotes. Following their commentary, Recital 2 of the Data Protection Directive underscores this general objective when providing for:

> "*Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;*"

The GDPR, which will succeed the Data Protection Directive, will enter into force in May 2018. Despite repeating certain elements of the paragraph above, there is, however, a shift of connotation in Recital (4):

> *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties* […]."

Whereas in the Data Protection Directive it was the data-processing systems which had to respect individuals' fundamental rights and freedoms, it is now the regulation, which has to respect all fundamental rights and observes freedoms and principles of the Charter. This would be alarming were the preamble of EU legislation having a binding legal force, which it has not.[22] The GDPR maintains as a broad objective that "*[t]his regulation protects fundamental rights and freedoms of natural persons"* but replaces the particular reference to the fundamental right to privacy with a reference to the right to the protection of personal data (Article 1(2) GDPR). Hence, the European legal culture on the protection of individuals' privacy and personal data has

[19] Rapport de la Commission Informatique et Libertés I, p. 19f.
[20] Article 1 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 1995 (OJ L281/31). See also the recurring references to '(fundamental) rights and freedoms' and 'the right to privacy' as separate concepts in the recitals to the Directive.
[21] Dammann and Simitis (1997), 101.
[22] EU Court of Justice, Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn), C-162/97, ECLI:EU:C:1998:554, para. 54; EU Court of Justice, Inuit Tapiriit and Others v European Commission, European Parliament, Council of the European Union, C-398/13 P, ECLI:EU:C:2013:625, para. 64.

always pursued to facilitate other fundamental rights and freedoms. The following section sets out to explain how this enabling function is recognised in EU law.

2.3 The enabling function of privacy and data protection in the EU

This section will explain how in the 'golden age of personal data' regulating the processing of an individual's personal data can be a proxy of intervention, which directly or indirectly could benefit other individual rights and freedoms. The focus we apply in this section is on the enabling function for individual rights and freedoms and we leave collective rights and democratic values, however important, aside. In the following we will explain the enabling function in relation to individuals' right to personal autonomy and integrity, freedom of expression, and how regulating the processing of personal data vests protection against discrimination, all of which are essential ingredients for the enjoyment of human dignity.

The rights that protect people's private life, thoughts, choice and expression, all operate within the sphere of human dignity. Together with human freedom, respect for human dignity is, in the words of the ECtHR, the "*very essence of the Convention*".[23] Also the EU "is founded on the indivisible, universal values of human dignity, freedom, equality"[24] and human dignity is protected as an "inviolable right" by the Charter.[25] Personal autonomy can be described as individuals' capability to choose how to live their own lives.[26] As a principle it is considered to be a meta-value behind a number of individual fundamental rights and freedoms.

It has been argued that the continental (European) privacy protections are in essence protections of human dignity and personal autonomy.[27] Both offer normative underpinnings of the fundamental rights to privacy and the protection of personal data and are foundations for other fundamental rights and values, which safeguards a sphere of individual choice and freedom. The close relationship between the right to privacy and personal autonomy comes to the fore in the jurisprudence of the ECtHR.[28] The objective to preserve personal autonomy influences the interpretation of the guarantees of the Convention's right to privacy.[29] The ECtHR has even stated that there is a right to personal autonomy included in Article 8 ECHR.[30] In German constitutional law, the fundamental right to informational self-determination is derived from the protection of human dignity.[31]

Personal autonomy is also a key rationale for instruments in EU data protection legislation, evidenced by for example the principles of consent and the individuals' right to access that aim to confer essential tenets of

[23] European Court of Human Rights 22 November 1995, case 20190/92, CR v UK, para. 42.
[24] See the preamble of the Charter of Fundamental Rights of the European Union.
[25] Article 1 EU Charter of Fundamental Rights (n 3).
[26] Koffeman (2010), 56. (Personal) Autonomy can be defined in many ways, see for example Dworkin (1988), 3–6, 20. This chapter follows the conceptualisation based on the case law of the ECtHR.
[27] Whitman (2004), 1161; Rössler (2005); Bernal (2014).
[28] Rainey / Wicks / Ovey (2014), 383.
[29] European Court of Human Rights 29 April 2002, case 2346/02, Pretty v UK, para. 61.
[30] European Court of Human 10 April 2007, case 6339/05, Evans v UK, para. 71; European Court of Human Rights 24 September 2007, case 5410/03, Tysiac v Poland, para. 107; European Court of Human 7 May 2009, case 3451/05, Kalacheva v Russia, para. 27.
[31] BGH, Urteil v. 15 Dezember 1983, I BvR 209, 269, 362, 420, 440, 484/83.

control over someone's personal data and means to influence the consequences of the processing of those data. The following account offers examples on the enabling effect of personal data protection legislation for the fundamental rights on freedom of expression, on freedom of thought and the prohibition of discrimination as protected by the ECHR and the EU Charter.

To begin with, the freedom of expression is guaranteed in Article 10 of the ECHR and Article 11 of the Charter. Freedom of expression does not only encompass the right to disseminate information; it also covers the right to hold opinions and freely receive information and ideas. However, today's prevalent monitoring of individual's viewing habits, tracking of online behaviour and extensive profiling could clash with the admittedly negative right to freely receive information. Because users are no longer free to inform themselves without being tracked, this can create a chilling effect for "freely" seeking information. The Court of Justice of the European Union has acknowledged that surveillance, whether by governments or companies, constitutes a serious interference with the fundamental rights to privacy and data protection that has a potentially chilling effect on the freedom of expression.[32]

With a view to protecting personal autonomy and the right to hold opinions, certain contemporary challenges are not about producing a chilling effect but about personal data-driven techniques of persuasion. Individuals increasingly face personalised messages by private actors but also political organisations, which are designed to persuade and may aim to manipulate individuals' actions from buying new goods and services to castings a vote in democratic elections. Such purposes for the processing of personal data may not be legitimate or require the individual's explicit consent. However, it is also clear that there is an important threshold for the protection of personal autonomy and the right to hold opinions that would be crossed by practices that are effectively manipulation.

An alternative angle to approach these challenges could be the freedom of thought, conscience and religion, which is guaranteed in Article 9 ECHR and Article 10 of the Charter. To date, the relevance of this fundamental right is manifest in protecting religious freedom and – narrowly interpreted - personal convictions.[33] However, as the amount of personal data that is collected about people and their online behaviour increases, so do the possibilities to analyse these data and discover (new) meanings in them.[34] In the future, ways to learn people's thoughts and convictions and to influence them are becoming more advanced, which may become a new frontier for privacy and data protection's facilitative function and trigger a renaissance of the fundamental right to freedom of thought.[35]

Personal data processing may lead to various forms of discrimination, intentional or not.[36] Discrimination on grounds such as race, religion, ethnic origin or gender is prohibited by Article 14 of the ECHR and Article 21 of the Charter. Data protection laws can help to mitigate discriminatory practices. This is achieved through giving

[32] EU Court of Justice, Digital Rights Ireland, C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 28, 37.
[33] Harris / O'Boyle / Bates / Buckley (2014), 592–594.
[34] On data production and possibilities for analysis in general, see OECD (2015), 133–161. For profiling, see Hildebrandt (2008).
[35] Bublitz (2014), 1-25.
[36] Custers / Calders / Schermer / Zarsky (2013).

individuals control over their personal data and vesting higher protection for special categories of personal data, i.e. "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*" (Article 8 (1) Data Protection Directive and Article 9 GDPR). The right to privacy also covers certain practices that are closely related to discrimination, such as the negative stereotyping of certain groups.[37]

Recognizing the enabling function of the fundamental rights to privacy and personal data protection has been close to visionary in the early 1980s. In the light of new data-intensive technologies the aforementioned risks are likely to grow and situations will arise that will require of Courts to more clearly argue the enabling functions. In the next step, we become even more concrete when using the contexts of big data and algorithmic decision-making to illustrate the intrinsic connection with individuals' fundamental rights and freedoms other than the rights to privacy and personal data protection.

3 Big data, algorithmic decision-making, and interferences with individual rights and freedoms

2.1 Big data and algorithmic decision-making

This section uses big data and algorithmic decision-making as a case study to *a)* illustrate how data processing can affect different individual fundamental rights and freedoms, and *b)* show the potential and limitations of the enabling function of the right to data protection, in the guise of contemporary EU data protection law. We commence by explaining the concept of big data and algorithmic decision-making, after which we elucidate its potential effects on individual rights and freedoms. We conclude the section by mapping out how EU data protection law addresses these issues, which is then evaluated in discussion in the ensuing section.

'Big data' has become a catch-for-all applications that involve very large quantities of (personal) data,[38] which are analysed to derive knowledge from it and then used to either target individuals or groups or make general information-based decisions. Big data can thus be regarded as a process consisting of three phases: acquisition, analysis, and application.[39]

[37] European Court of Human Rights, 15 May 2012, cases 4149/04 and 41029/04, Aksu v Turkey, para. 58.
[38] Occasionally big data is based on data that do not relate to individuals, such as meteorological data, logistical data, or data about production processes, but often personal data processing is involved.
[39] Oostveen (2016).

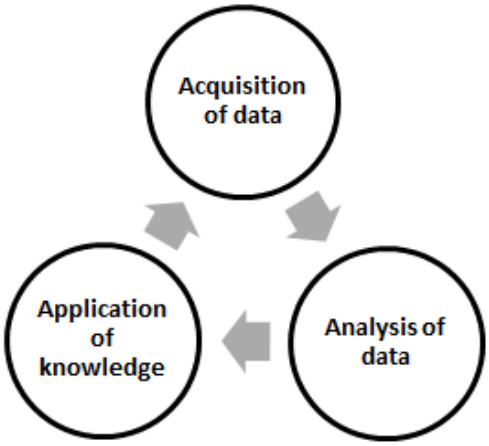

Figure 1: big data process

In the first phase an organisation collects or acquires (personal) data. Personal data can be collected from individuals directly, for example when a social networking platform ask users to provide them with information. Personal data can also be acquired from data brokers, companies that collect data with the core purpose of selling them to third parties. A third possibility of acquiring data is combining existing datasets, such as personal data on physical fitness with shopping behaviour, to create new data.

In the second phase of big data, the data is analysed to be able to derive knowledge from it and create for example models or predictions on probabilities of defaulting on payments. The techniques that are used are constantly changing.[40] They include machine learning, which facilitates open-ended explorations for patterns, without clear prior questions or hypotheses being necessary.[41]

In the final phase, the knowledge is applied and algorithmic decisions are made. Based on the models, predictions or knowledge, individuals can be categorised or clustered, to for example show them different advertisements or decide what interest they should pay for loans. What is important here, is to realise that the algorithmic decision is not made on the basis of solely the data from that targeted individual. The decision rests on a limited amount of personal data from this individual, but behind that decision is a wealth of data from other people or sources. The millions of data that are collected and analysed to *create* the knowledge, models or predictions, are in principle unrelated to the data that are used to *apply* the knowledge, models or predictions in the application phase of big data.

It is also possible that people are not targeted as individuals or groups, but that general decisions are taken that affect their individual's lives nonetheless, such as when governments base policy decisions on big data analytics. The ensuing subsection explicates the immediate effects of big data and algorithmic decision-making and the resultant long-term interferences on individual rights and freedoms.

[40] Custers (2013), 7.
[41] Calders / Custers (2013), 31–38.

2.2 Interferences with individual rights and freedoms

Undoubtedly, big data as described above can interfere with the rights to privacy and data protection, because of the large-scale collection of personal data and the effect that the processing can have on the private life of individuals. As the collection and processing of personal data intensify and the means to extract knowledge become more sophisticated, the possible spectrum and intensity of interferences increases. However, as this chapter is about the enabling function of privacy and data protection, we here focus on big data's detrimental effects on individual rights and freedoms other than privacy and data protection.

First of all, the means used to gather individuals' personal data, how the data are processed, and the lack of transparency surrounding it, can exert pressure on the personal autonomy and informational self-determination of the individual.[42] Targeting individuals with personalised communications feeds the fear that they will end up in filter bubbles or information cocoons, which would isolate them in a world that consists of limited information that always confirms their beliefs and opinions, without being exposed to diverging information and viewpoints.[43] Whereas people may think they make independent choices and form their opinions autonomously, in such circumstances they are in fact influenced by the limited and customised information that is offered to them. Additionally, people could also be actively persuaded or manipulated through personalisation strategies. Both limiting choices and information as well as actively persuading or manipulating people into a specific choice or decision, reduces individual's personal autonomy. Currently, the ways in which personalisation and the steering of opinions and behaviour may be small. But in spite of these instances being small or trivial in terms of their context, because of the opacity surrounding it and their cumulative effects, they could prove harmful for personal autonomy.

Second, big data and algorithmic decision-making can lead to – intentional or unintentional – discrimination.[44] Big data allows for ever more detailed categorisation of people and the customisation of the treatment of individuals. When individuals are treated differently than others on the basis of race, sex, religious beliefs, or other characteristics listed in the Convention and the Charter,[45] this is direct discrimination. But in addition to discrimination on the basis of prohibited characteristics, big data can cause a more covert kind of discrimination: a seemingly innocent correlation can be a *proxy* for discrimination. This is easily explained through the example of redlining. Redlining refers to the practice in which particular areas or neighbourhoods are denied services, which in practice comes down to denial of services to people of a certain ethnic background as they are the group living in that (generally poor) residential area, leading to discrimination on ethnic grounds.[46] The neighbourhood serves as a proxy for ethnicity. Similarly, correlations in big data can be proxy's for prohibited discrimination characteristics. Basing decisions on variables such as pet breed or type of car or dietary requirements may seem innocuous, but they are not if they correlate to ethnic group or religious beliefs. This

[42] Richards / King (2013), 42–43.
[43] Pariser (2012). However, so far no clear evidence about the existence of filter bubbles has been found, see Zuiderveen Borgesius / Trilling / Möller / Bodó / de Vreese / Helberger (2016).
[44] For an extensive (US) analysis, see Barocas / Selbst (2016).
[45] Article 21 European Convention on Human Rights (n 2); Article 14 EU Charter of Fundamental Rights (n 3).
[46] Barocas / Selbst (2016), 689–690.

kind of 'hidden' discrimination is more difficult to uncover than direct discrimination, particularly as numerous variables are used for complex data analysis, as is the case in big data.

The rights to freedom of expression and, potentially, thought are affected by big data in a variety of ways, in different phases of the big data process. As explained above, when people have the feeling that they are under surveillance, be it governmental or corporate, they may alter their behaviour.[47] Surveillance's chilling effect is easily recognised; the mere collection of large amounts of data can be sufficient to affect individuals' right to freely seek and impart information. But freedom of expression also encompasses the rights to hold opinions and to free reception of information and ideas, and these rights could be compromised by extensive personalisation. Specific characteristics place individuals in groups, which in-or excludes them from certain information in the third phase. This potentially limits opportunities to find (new) information and developing ideas and beliefs, which is closely linked to reduced autonomy as described above. The possible harmful effects of big data on freedom of expression and thought thus work two ways: people may self-censor their expression, and their free, unhindered reception of information and forming of thoughts and ideas may be hindered.

In sum, big data and algorithmic decision-making pose risks for a several individual rights and freedoms, not just to the rights to privacy and data protection. It has many effects on different rights and freedoms, that occur throughout the whole process, which is summarised in figure 2 below.

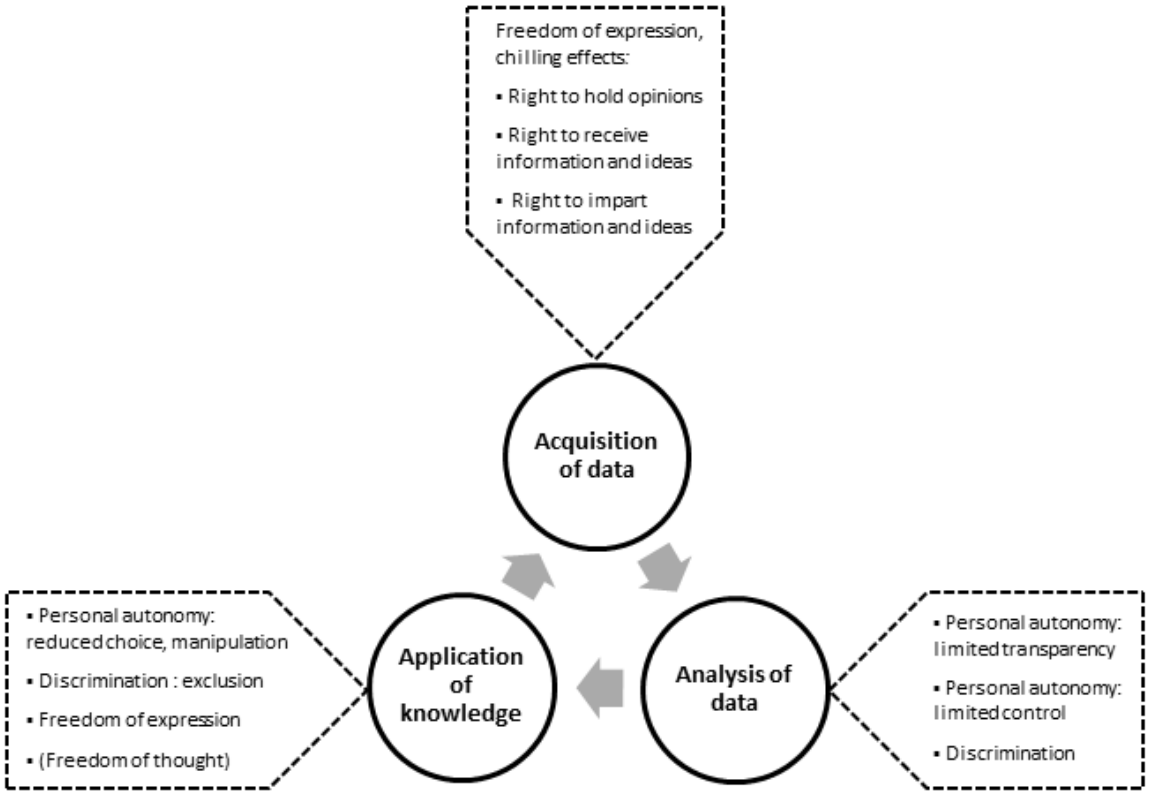

Figure 2: big data process including effects on individual rights and freedoms

[47] Richards (2012), 1940–1941, 1952–1953.

But data processing can also affect the lives of individuals *after* the initial processing has occurred. The potential effects of big data, and data processing in general, should be seen as a cascade: it starts with data protection law and privacy, but further in the process the consequences become more far-reaching for other individual rights and freedoms. This is also what we mean when referring to the 'long-term interferences' of personal data processing. The long-term interferences connotes that every instance of personal data processing as applied in automated decision-making alters the course of events, even if at first sight insignificantly, and may yield not only short-term effects, but also long-term interferences. An example of long-term effects: not admitting an applicant to study medicine will inevitably preclude her from becoming a medical doctor in her later life. Thus, the decision changed the course of her career irrevocably and in doing produces additional effects, such as for example lower income prospects, which will influence the mortgage available to her, etc.[48]

The effects of personal data collection and processing permeate further individual's life in ways that affect personal autonomy, with significant risks of interfering with individual rights and freedoms across the spectrum, risks that were probably unforeseen at the time of collection. In regulating the beginning of the cascade of effects, the point where personal data are collected and further processed, data protection law has the protective potential. The discussion of data protection law's protective potential starts in the following subsection, that summarizes what data protection has to offer in the context of (big) data processing and algorithmic decision-making.

2.3 EU data protection law

EU data protection law is composed of key concepts, e.g. the definitions of personal data and individual consent, principles relating to data quality and the requirement for a legal basis for legitimate processing of personal data. The GDPR by and large continues the regulatory approach that has been in place since the Data Protection Directive, such as instituting mechanisms of individual's control over their personal data and remedies. However, as a EU regulation the GDPR will be binding and directly applicable in the Member States (Art. 288 TFEU).

EU data protection law protects individuals' fundamental rights and freedoms by providing them with means to control their personal data, mainly through mandating transparent information and data subject rights. Transparency is achieved by requiring organisations that process personal data to provide the individual with various kinds of information, on for example its identity, the type of data processed and the purposes of such processing.[49] The rationale is that this information should enable individuals to assess the intended processing of personal data up front from entering into a commercial transaction or being asked for consenting to the processing of their personal data. The right to object to processing and the emphasis on consent as a basis for legitimate personal data processing,[50] should enable the individual to set her personal boundaries and differentiate according to data type, organization or processing-context.

[48] Herpel (2016).
[49] Articles 13-15 GDPR.
[50] Articles 21 and 6-7 GDPR.

In the big data process such means to control the use of one's personal data provide a certain sphere of personal autonomy in that the individual can choose not to be part of a given data processing operation. Moreover, the targeting or personalization of the application phase can be avoided, although a denial of services may be the result. As such, the control over personal data offered by data protection law addresses the chilling effect that processing can have on freedom of expression and personal autonomy. Further interferences with individual fundamental rights and freedoms are addressed through opportunities to learn about and refuse automated decision-making and, to some extent, personalisation in the application phase.

The provision on automated individual decision-making, including profiling, in Article 22 GDPR has the crucial function to mitigate the risks of big data and automated decision making for individual rights and freedoms. The GDPR's rules on automated individual decision-making are a prime example of enabling individuals to control their personal data and have agency in the context of automated decision-making. The core of these rules is the right to refuse to be subjected to automated decisions, which already existed in the Data Protection Directive. In the GDPR the rules are expanded, most prominently by adding 'profiling' to the provision.[51] Summarising, the GDPR contains five main rules on profiling and automated-decision making: 1) the controller's *obligation to provide information*, 2) the data subject's *right of access to information*, 3) the data subject's right to *object to personal data processing*, 4) the data subject's right to *oppose automated individual-decisions*, including profiling, and 5) the *prohibition* on automated decision-making based on *special categories of personal data*.

There clearly is much potential in the combination of information duties with the rights to object and the right not to be subjected automated decision-making, including profiling, for individual rights and freedoms in big data. Through providing individuals with information and giving them the right to object to the processing of personal data as well as automated decisions or evaluative measures, personal autonomy is strengthened. Individuals have the possibility to decide whether they want to be evaluated or treated differently on the basis of personal aspects, which protects against manipulation. Furthermore, they can demand human intervention in the decision making process, express their views and challenge the decisions.[52] This right to be heard and judged by humans instead of machines moreover reflects a respect for human dignity. The general possibilities to object and contest decisions, but in particular the prohibition of profiling and decision-making on the basis of special categories of data, can counter instances of direct discrimination in the application phase.

But data protection law is not solely about control and rights of individuals. It is also about obligations of the people or organizations who process the data, and general prohibitions. For example, as explained earlier discrimination risks are also mitigated by data protection's limitations on the processing of special categories of personal data, such as data on health, ethnicity or religious views.[53] Furthermore, on the basis of the new rules of the GDPR, big data organizations are in principle required to carry out data protection impact assessments, containing amongst others descriptions of data flows, risks, safeguards and security measures.[54] Organizations are also under the obligation to take appropriate technical and organisational measures to protect the rights of

[51] Article 22 GDPR.
[52] Article 22 (3) GDPR.
[53] Article 9 GDPR.
[54] Article 35 (3) (a) and (7) GDPR.

data subjects. Non-compliance with these provisions is subject to administrative fines.[55] These obligations make organizations aware and responsible for actively safeguarding individuals rights in practice. How far these duties stretch, and how the general potential of data protection law's facilitative role for other individual rights and freedoms plays out in practice, is discussed in the ensuing section.

4 Discussion of data protection law's contribution to protecting individual rights and freedoms

It is apparent from the previous section that EU data protection law not only protects the rights to privacy and data protection, but that it has the capacity to also facilitate the protection of other individual rights and freedoms, notably personal autonomy, non-discrimination, freedom of expression and thought, and therefore ultimately, human dignity. Because of the obligation to inform individuals when their personal data are processed and how this processing takes place, the process should be transparent. Individuals are given elementary tenets of control over their personal data, especially where their consent to the processing activity is required, but importantly also the right not to be subjected to automated decision making, including profiling. At the same time, organizations must assess their processing to determine risks and precautions, and they are therefore forced to take individuals' rights and interests into account before processing their data. Administrative fines and individual remedies back up these obligations.

Yet, aside from these strong tools, there are a number of weaknesses in the legal data protection framework. To begin with, the scope of data protection law is limited to personal data, data that relate to natural persons that are identifiable through the data.[56] Personal data can be anonymised or non-personal, which also makes their processing unregulated, but their combination with other (personal) data can affect the lives of individuals.[57] If in general decisions are made in the application phase, algorithmic decisions that do not target individuals but affect their lives nonetheless, it is also beyond the scope of data protection law. In such cases the acquisition and analysis phases could be covered because identifiable data can be processed. But as the phases are disconnected and the personal data are acquired from other people in the first and second phase instead of from the individual in the third phase, this affected individual cannot rely on data protection law.

Second, there is scepticism about individual control over data processing as a protection mechanism. Often in a digital environment,[58] but particularly in the context of big data, it is doubtful whether transparency obligations work. Because contemporary personal data processing is ubiquitous and complex, is questionable whether organizations are always able to adequately inform data subjects about personal data processing, and whether data subjects are capable of assessing the consequences thereof.[59] Moreover on the internet individuals often

[55] Article 83 (5) (a), (4) (c) GDPR.
[56] Article 4 (1) GDPR.
[57] Oostveen (2016).
[58] Acquisti (2010); Irion / Luchetta (2013), 35f.
[59] See for example Barocas / Nissenbaum (2014), 2.

face a monopolist, and a denial of services if they do not agree with the conditions regarding personal data sharing. This constrains free choice, or even makes it impossible.[60] Faced with for example the automatic refusal of a loan or the impossibility of connecting to others on networks, individuals may easily agree with personal data processing that could lead to discrimination or reduce personal autonomy.

And even if people are offered and have absorbed all information, they still make choices in practice that they claim not to agree with.[61] Reasons are amongst others being tempted by benefits (like being allowed to visit a website, using a service, receiving discounts, or using free apps), not being able to oversee the long-term consequences, or resignation in the idea that privacy and data protection on the internet are a lost cause.[62] People may have tools to prevent discrimination or chilling effects, and increase personal autonomy, but they may simply not command them. One of the limitations is that privacy management has become a herculean task for individuals almost impossible to fit into the routines of personal life: reading privacy notices, entering privacy preferences, managing updates in organisation's privacy notices and keeping an general overview over which organisation is processing their personal data for which specific purposes, in addition to being inclined to exercise data subjects rights or turn to the competent data protection authority.[63]

The potential of the automated decision-making rules is limited, as they only apply when a decision has legal effect or when individuals are *similarly significantly affected* by the decision. Second, the decision must be fully automated, i.e. no human must have played a part in the decision-making process for Article 22 to apply. This means that in practice people's lives may be governed by much small and seemingly insignificant algorithmic decisions-making, which would, as explained in subsection 2.2, interfere with personal autonomy, without possible recourse on the basis of Article 22 GDPR. Also, when substantial decisions are based on big data analysis but not applied through automated means, as would be the case when someone is fired on the basis of big data,[64] Article 22 provides no recourse. In the bleakest scenario, the definition of 'profiling' of Article 4 (4) GDPR creates another obstacle for the application of Article 22 in the context of big data. Part of the profiling definition is "*the use of personal data to evaluate certain personal aspects relating to a natural person*". And as explained above, the data in the analysis phase often does not qualify as *personal* data. Thus, if the definition of profiling of Article 4 (4) would be interpreted narrowly, most big data applications would be beyond the scope of Article 22 *per se.*

It appears to us that the key principles and procedural rights of individuals, which have been established substance of the EU data protection law since its inception, are more potent to mitigate the long-term risks of big data and algorithmic decision-making compared to the specialised provisions on automated decision-making and profiling in the GDPR. The reason is that key principles and procedural rights of individuals are generic whereas the special rules may not meet big data practice.

[60] Bygrave / Schartum (2009), 160.
[61] Acquisti (2010), Irion / Luchetta (2013), p. 36f.
[62] Tene / Polonetsky (2013), 67; Rouvroy (2016), 23.
[63] Solove (2013).
[64] O'Neil (2016), 3-11.

5 Conclusion

Where personal data processing is concerned, the discussion of fundamental rights protection often centres around privacy and data protection. After all, these fundamental rights have the most direct connection to the data processing in practice, and the interferences of these rights by data processing are generally quite visible. However, new technologies and data processing applications can affect a range of individual fundamental rights and freedoms, which can subsequently have long-term effects on people's lives.

The protection of privacy and personal data processing with a view on its enabling function for other individual fundamental rights and freedoms has been ingrained in constitutional law in Europe for years, yet this link has not received much attention in the European legal discourse. We deem that this enabling function of privacy and data protection should gain more attention, because of how new data processing developments such as big data and algorithmic decision-making can interfere with individual fundamental rights and freedoms other than privacy and data protection, and the lasting effect this can have on individuals' chances and future. Understood as an enabling right, the architecture of EU data protection law is capable of serving as a proxy for the protection of other individual fundamental rights and freedoms, especially where it provides for appropriate default situations for the handling of personal data, such as requiring a legal basis and a specific purpose or granting rights to data subjects. The new GDPR certainly strengthens aspects of this core architecture by requiring more accountability of compliance with personal data protection standards.

Ironically, certain regulatory innovations brought by the GDPR to cope with technological advancement and the data-driven economy appear less capably of yielding broad protection for individuals fundamental rights and freedoms. This chapter discussed the provisions on automated individual decision-making and profiling, the requirements of which are too narrowly circumscribed to meet the state of the art big data applications. Requiring personal data as an input limits the application of these specific provisions even though automated-decisions are made and individual profiles are created. It seems that the GDPR's specific innovations may not yield as much of an enabling function than what general data protection regulation achieves anyhow.

In general, an enabling effect emanates from the GDPR, for example through the control that is bestowed upon individuals with respect to their personal data, and through special protection for sensitive data. However, in practice these effects may be undermined by context-specific barriers. In addition to the examples given above, such as the herculean task of personal online privacy management,[65] it remains to be seen how the GDPR's standards will work in practice. There is always the risk that the envisaged active protection of individual's rights and freedoms of the law, turns in to 'check-boxing' and hiding behind formalities in practice.[66] Moreover, data protection authorities' capacities and power to monitor the whole digital personal data processing ecosystem should not be overestimated. Too much optimism in this area equals a lack of attention for the lacunae in the framework of protection of individual rights and freedoms.

[65] Solove (2013).
[66] As an example, see how privacy policies are currently often used: they become are long, complicated, vague, and almost incomprehensible texts, that seem to be written with compliance and liability in mind, instead of with aim to provide clear information to data subjects. See Kuner / Cate / Millard / Svantesson (2012), 68.

In sum, even with privacy and data protection having their stand-alone value and their function as enabling rights, it is about time to review possible alternative approaches to the effects of processing personal data. From the perspective of individual rights and freedoms, it is worthwhile to explore how other (legal) approaches can complement privacy and data protection in their protection of individual rights and freedoms in the context of personal data processing. Regulating data processing neutralizes part of the negative effects that data processing can have on individual fundamental rights and freedoms, but for the long-term effects on individuals' lives, it is simply not enough.

Reference list

Acquisti, A., The Economics of Personal Data and the Economics of Privacy, Background Paper for OECD Joint WPISP-WPIE Roundtable, 1 December 2010, Paris

Barocas, S. / Nissenbaum, H. (2014), Big Data's End Run Around Procedural Privacy Protections: Recognizing the inherent limitations of consent and anonymity, Communications of the ACM, 31

Barocas, S. / Selbst, A. (2016), Big Data's Disparate Impact, California Law Review 2016, 671

Bernal, P. (2014), Internet Privacy Rights: Rights to Protect Autonomy, Cambridge University Press

Brownsword, R. (2014), Human Dignity from a Legal Perspective, in: The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives, Cambridge University Press

Bublitz, J.C. (2014), Freedom of Thought in the Age of Neuroscience, Archives for Philosophy of Law and Social Philosophy 2104, 1

Bygrave, L. / Schartum, D.W. (2009), Consent, proportionality and collective power, in: Reinventing Data Protection?, Springer

Calders, T. / Custers, B. (2013), What Is Data Mining and How Does It Work? In: Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer

Custers, B. (2013), Data Dilemmas in the Information Society: Introduction and Overview, in: Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer

Dammann, U. / Simitis, S. (1997), EG-Datenschutzrichtlinie: Kommentar, Nomos Verlagsgesellschaft

Dworkin, G. (1988), The Theory and Practice of Autonomy, Cambridge University Press

González Fuster, G. (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing

Harris, D. / O'Boyle, M. / Bates, E. / Buckley, C. (2014), Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights, Oxford University Press

Herpel, W. (2016), Chaotische Studienplatzvergabe sorgt für Frust, Spiegel Online of 26 June 2016, available at: www.spiegel.de/lebenundlernen/uni/nc-faecher-studienplatz-vergabe-frustriert-studenten-a-1099120.html

Hildebrandt, M. (2008), Defining profiling: a new type of knowledge?, in: Hildebrandt, M. and Gutwirth, S. (eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer

Irion, K. / Luchetta, G. (2013), Online Personal Data Processing and the EU Data Protection Reform, Centre for European Policy Studies, 2013, available at: http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform

Koffeman, N. (2010), (The right to) personal autonomy in the case law of the European Court of Human Rights, Leiden University

Krotoszynski, R. (2016), Privacy Revisited: A Global Perspective on the Right to be Left Alone, Oxford University Press

Kuner, C. / Cate, F.H. / Millard, C. / Svantesson, D.J.B. (2012), The challenge of "Big Data" for data protection, International Data Privacy Law, 47

Lynskey, O. (2014), Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order, International and Comparative Law Quarterly, 569

OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing

O'Neil, C. (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown

Oostveen, M.A.A. (2016), Identifiability and the applicability of data protection to big data, International Data Privacy Law 2016, available at: idpl.oxfordjournals.org/content/early/2016/09/06/idpl.ipw012.full

Pariser, E. (2012), The Filter Bubble, Penguin Books

Rainey, B. / Wicks, E. / Clare, O. (2014), Jacobs, White and Ovey: The European Convention on Human Rights, Oxford University Press

Reh, H.J. (1978), Kommentar zum Bundesdatenschutzgesetz, in Simitis, Dammann, Mallmann and Reh, Kommentar zum Bundesdatenschutzgesetz, Nomos

Simitis, S. / Dammann, U. / Mallmann, O. / Reh, H.J. (1978), Kommentar zum Bundesdatenschutzgesetz, Nomos

Richards, N. (2015), Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Oxford University Press

Richards, N. (2012), The Dangers of Surveillance, Harvard Law Review 2012, 1934

Richards, N. / King, J. (2013), Three Paradoxes of Big Data, Stanford Law Review 2013, 41

Roberts, J.L. (2015), Protecting Privacy to Prevent Discrimination, William and Mary Law Review 2015, 2097

Rössler, B. (2005), The Value of Privacy, Polity Press

Rouvroy, A. (2016), Of Data And Men: Fundamental Rights and Freedoms in a World of Big Data, Bureau of the Consultative Committee of the Convention for the Protecion of Individuals with Regard to Automatic Processing of Personal Data [ETS 108]

Solove, D.J. (2013), Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, 1880

Solove, D.J. (2008), Understanding privacy, Harvard University Press

Solove, D.J. (2006), A Taxonomy of Privacy, University of Pennsylvania Law Review 2006, 447

Tene, O. / Polonetsky, J. (2013), Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 2013, 239

Tzanou, M. (2013), Data protection as a fundamental right next to privacy? “Reconstructing” a not so new right, International Data Privacy Law 2013, 88

Whitman, J. (2004), The Two Western Cultures of Privacy: Dignity versus Liberty, Yale Law Journal 2004, 1151

Zuiderveen Borgesius, F. J. / Trilling, D. / Möller, J. / Bodó, B. / de Vreese, C. H. / Helberger, N. (2016), Should we worry about filter bubbles?, Internet Policy Review 2016, 1