Meaningful Transparency through Data Rights: A Multidimensional Analysis

Naudts, L.; Dewitte, P.; Ausloos, J.

DOI
10.4337/9781800371682.00030

Publication date
2022

Document Version
Final published version

Published in
Research Handbook on EU Data Protection Law

21. Meaningful transparency through data rights: A multidimensional analysis

Laurens Naudts, Pierre Dewitte and Jef Ausloos

1. INTRODUCTION

1.1 Transparency in a Digital Society

We are increasingly governed through data, and getting insight into how data infrastructures affect the way we learn, work and live becomes ever more important. Gig economy workers, for instance, are often entirely at the mercy of algorithmic governance by their respective platform, with little to no understanding of, or means to challenge, such automated decision-making.[1] In recent years, these – often low-paid – workers have tried to push back in order to enforce better labour conditions.[2] Access to their data as well as information on how they are used, can play

[1] Ryan Calo and Alex Rosenblat, 'The Taking Economy: Uber, Information, and Power' (2017) 117 *Columbia Law Review* 1623.

[2] For example, in a series of cases in March 2021, the Dutch District Court of Amsterdam ruled in favour of (digital) rights for so-called gig drivers. More specifically, the Court ordered Uber and Ola, two gig-economy platforms, to be more transparent regarding the mechanisms and data through which they score and profile their drivers. The Court's rulings demonstrate among others the complementary and practical importance data transparency rights can have in safeguarding (digital) rights (See also sections 2, 3 and 4 of this chapter, and further observations at nn. 87, 93, 111, 117 and 161). See: Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1018; https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1018 accessed 23 June 2021; Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019; https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019 accessed 23 June 2021; Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1020; https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020 accessed 23 June 2021. For more information, including an unofficial translation of the aforementioned cases into English, see: Ekker Legal, 'Dutch court rules on data transparency for Uber and Ola drivers.' (*Ekker Legal,* 13 March 2021) https://ekker.legal/2021/03/13/dutch-court-rules-on-data-transparency-for-uber-and-ola-drivers accessed 23 June 2021; App Drivers & Couriers Union, 'Gig Economy Workers score historic digital rights victory against Uber and Ola Cabs' (12 March 2021), https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs accessed 23 June 2021; 'Q&A: Fighting for Workers' Right to Data' (*Open Society Foundations - Voices*, 23 May 2019) https://www.opensocietyfoundations.org/voices/q-and-a-fighting-for-workers-right-to-data accessed 10 November 2020; Laura Kayali, 'Drivers Take Legal Action against Uber to Demand Their Data' *POLITICO* (20 July 2020) https://www.politico.eu/article/drivers-take-legal-action-against-uber-to-demand-their-data/ accessed 17 August 2020; 'Uber drivers demand access to their personal data' (*Ekker Advocatuur*, 19 July 2020) https://ekker.legal/2020/07/19/uber-drivers-demand-access-to-their-personal-data/ accessed 17 August 2020; Jill Toh 'Empowering Workers Through Digital Rights'. *Digital Freedom Fund*, 30 April 2021 https://digitalfreedomfund.org/empowering-workers-through-digital-rights/ accessed 17 August 2020.

a vital role in these endeavours.[3] Similarly, the last years have seen a surge in efforts to make (news) recommender systems more transparent in order to safeguard democratic values such as (media) pluralism and prevent the spread of disinformation.[4] Data rights have played an important role in several of these efforts. Aside from constituting valuable tools in these battles for social justice or public values, data rights may also be curiosity-driven with people simply wanting to better understand how and for what purposes their data are being processed. These attempts to make digital infrastructures more transparent are symptomatic of the broader need to empower individuals and society and realign information-driven power asymmetries.

The importance of transparency with regard to the processing of personal data has been solidified in Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter CFR).[5] Having enshrined key data protection principles such as fairness, purpose specification, lawfulness and the rights of access and to rectification, a teleological reading of the CFR suggests that the processing of personal data should be accompanied by robust transparency standards.[6] The fundamental right to personal data protection is inherently tied to the challenges raised by the datafication of society, and safeguard autonomy and freedom from being curtailed by the processing of personal data.[7] Yet, the processing of personal data affects more than just autonomy, freedom or self-determination; it can also have impact on

---

[3] Beyond the cases mentioned under (n 2), for more examples and theorisation, see: René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020) https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487 accessed 7 July 2020.

[4] Jef Ausloos, Paddy Leerssen and Pim ten Thije, 'Operationalizing Research Access in Platform Governance What to Learn from Other Industries?' (2020) https://algorithmwatch.org/en/governing-platforms-ivir-study-june-2020/#study accessed 26 November 2021; Max van Drunen, Natali Helberger and Mariella Bastian, 'Know Your Algorithm: What Media Organizations Need to Explain to Their Users about News Personalization' (2019) 9 *International Data Privacy Law* 220; Nava Tintarev, Shahin Rostami and Barry Smyth 2018, 'Knowing the Unknown: Visualising Consumption Blind-Spots in Recommender Systems', *Proceedings of the 33rd Annual ACM Symposium on Applied Computing* (ACM 2018) http://doi.acm.org/10.1145/3167132.3167419 accessed 21 February 2021; Luciana Monteiro Krebs, Oscar Luis Alvarado Rodriguez, Pierre Dewitte, Jef Ausloos, David Geerts, Laurens Naudts, and Katrien Verbert. 2019. Tell Me What You Know: GDPR Implications on Designing Transparency and Accountability for News Recommender Systems. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19). Association for Computing Machinery, New York, NY, USA, Paper LBW2610, 1–6. DOI:https://doi.org/10.1145/3290607.3312808.

[5] Charter of Fundamental Rights of the European Union [2000] OJ 2000/C, C364/1.

[6] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 *Yearbook of European Law* 130 https://academic.oup.com/yel/advance-article/doi/10.1093/yel/yey004/5068688 accessed 14 August 2018; Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC http://www.jipitec.eu/issues/jipitec-10-3-2019/5031 accessed 21 February 2021; P J A De Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' (2006) *Privacy and the Criminal Law* 61.

[7] Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020) 54–90.

access to information,[8] education,[9] work,[10] or equality and non-discrimination.[11] This is where the GDPR comes in. As a piece of secondary legislation, it is broader than Article 8 CFR and aims to ensure the protection of all interests, fundamental rights and freedoms in the context of personal data processing.[12] Put differently, the GDPR provides a tool for challenging data processing operations that affect any of our fundamental rights and freedoms.[13] The GDPR recognises the benefits of data processing, but also aims to prevent disproportionate impacts on both the individual and society.[14] It integrates fairness mechanisms in an effort to restore informational power asymmetries, introducing a requirement of lawfulness and granting individuals a set of powerful data rights.[15] Among these rights, and central to the current chapter,

---

[8] CFR, art 11. News recommender systems, for instance, increasingly curate the content delivered to online users. This can, in turn, exacerbate preferences that are voluntarily expressed by end-users. See: for a use case on the 2018 Italian elections: Eduardo Hargreaves and others, 'Biases in the Facebook News Feed: A Case Study on the Italian Elections' [2018] Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) 806.

[9] CFR, art 14. This is best illustrated by the recent backlash that followed the use of an algorithm to assess British students for university admission decisions amid the COVID-19 pandemic. See: Karen Hao, 'The UK exam debacle reminds us that algorithms can't fix broken systems' (2020) *MIT Tech Review* https://www.technologyreview.com/2020/08/20/1007502/uk-exam-algorithm-cant-fix-broken-system/ accessed 22 February 2021.

[10] CFR, art 15. Algorithmic decision-making processes are increasingly used to sort job applicants and monitor employee's behaviour and performance. In 2018, such practices led to the automated termination of Ibrahim Diallo's employment contract. See: Jane Wakefield, 'The man who was fired by a machine' (2018) BBC https://www.bbc.com/news/technology-44561838 accessed 22 February 2021.

[11] CFR, art 21, as well as more broadly, CFR arts 20–26. The discriminatory side-effects of data processing have been well-documented in (legal) literature. Examples include: Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact Essay' (2016) 104 *California Law Review* 671; Frederik J Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) *The International Journal of Human Rights* 1; Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6 *Big Data & Society* 2053951719895805; Laurens Naudts, 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them' in Ronald Leenes and others (eds), *Data Protection and Privacy : The Internet of Bodies* (1st edn, Hart Publishing 2019) http://www.bloomsburycollections.com/book/data-protection-and-privacy-the-internet-of-bodies/ch3-how-machine-learning-generates-unfair-inequalities-and-how-data-protection-instruments-may-help-in-mitigating-them/ accessed 21 February 2019; Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 *Journal of Big Data* 12.

[12] GDPR, art 1(2). Regulation 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 L119/1.

[13] Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020) 54–90.

[14] See (the many references in): Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?' (2014) 51 *Common Market Law Review* 843, 849.

[15] See in this regard: Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2016) 213; Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46 EC and the Proposed General Data Protection Regulation' 50 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf accessed 24 February 2021; Antoinette Rouvroy and Yves Poullet, 'The Right to Informational

the GDPR offers data subjects a set of multifaceted and versatile transparency rights that allow them to gain more insight into data processes, (re)capture control and equalise power dynamics in the digital society.

1.2 Structure, Research Objectives and Method

This chapter explores the role of the GDPR in achieving better transparency, establishing control and mitigating data-driven power asymmetries. The GDPR's transparency provisions vary in terms of detail (from generic[16] to specific[17]), timing (ex-ante[18] or ex-post[19]), audience (from data subjects[20] to supervisory authorities[21]) and initiation (pull versus push[22]).[23] The diversity showcased by the GDPR's transparency provisions – indicating both a multifaceted and polyvalent nature – has remained largely understated however.

We develop a framework through which we hope to reaffirm the unique nature of the GDPR transparency provisions. To do so, we focus on transparency obligations and information-related data subject rights, hereinafter referred to as 'data transparency rights',[24] which are found primarily in Articles 12, 13, 14, 15 and 22 GDPR.[25] For the purpose of our

---

Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 69 http://link.springer.com/10.1007/978-1-4020-9498-9 accessed 26 February 2021; Frits W Hondius, *Emerging Data Protection in Europe* (North-Holland 1975) 23 (also referring to the Hesse [pp 35–36] and Swedish [p 89] Data Protection Acts as specifically aimed at balancing power).

16 E.g., GDPR, art 5(1)a.

17 E.g., GDPR, art 15.

18 E.g., GDPR, arts 13–14.

19 E.g., GDPR, arts 15 and 20.

20 E.g., GDPR, arts 15 and 20.

21 E.g., GDPR, art 30(4).

22 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021.

23 Jef Ausloos and Michael Veale, 'Researching with Data Rights' (2020) *Technology and Regulation* 136 https://techreg.org/index.php/techreg/article/view/61 accessed 24 February 2021.

24 The key provisions we focus on can all be found under Chapter III of the GDPR: 'Rights of the Data Subject'.

25 For the purposes of our research, a comprehensive review of legislation, literature and case-law has been performed focusing primarily, albeit not exclusively, on those sources relevant to the understanding of the highlighted data transparency rights and the role and function ascribed to transparency within data protection. In doing so, we aimed our attention to the most direct and instrumental transparency provisions data subjects have access to under the GDPR. As a consequence however, other transparency provisions within the GDPR have been excluded from the current analysis, such as arts 20 (the right to data portability), 30 (records of processing activities) and 33–34 GDPR (data breach notifications). It can also be noted that this chapter was finalised before the publication of the European Data Protection Board's guidelines on the right of access, which were adopted in January 2022. See: European Data Protection Board, 'EDPB Adopts Guidelines on Right of Access and Letter on Cookie Consent' (19 January 2022) <https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-right-access-and-letter-cookie-consent_en> accessed 21 January 2022. Likewise, it should be recognised that the GDPR does not hold a monopoly on data (transparency) rights. As (EU) legislators are catching up with the digital revolution, a growing number of such rights can be found in other legal frameworks. See, e.g., art 16(4) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA

analysis, we consider the aforementioned provisions as data transparency rights because they grant data subjects a corresponding claim or right to obtain information. These prerogatives aim to provide data subjects with information about, and control over, the processing of their personal data. This chapter will evaluate how, and under what conditions, these rights can be effectively used by data subjects in the pursuit of transparency and transparency-related goals. In this sense, our approach is teleological: departing from the (protective) purposes and objectives underlying data transparency rights, the chapter will ascertain and evaluate the potential role and function these rights can have by capturing their range and value.

Throughout this chapter, we hope to demonstrate that data transparency rights not only advance transparency, but can also be exercised for a wide range of (sometimes more subtle) purposes. For example, transparency can be seen as a process that provides insight into data structures; insight which, in turn, can be used to regain control over said structures and even serve to mitigate asymmetries in power associated with them. Data transparency rights can play an important role in having those functions of transparency realised. Still, the degree of success with which data transparency rights are exercised might vary depending on the purpose one has.

The effectiveness of data transparency rights, we argue, hinges upon – at least – three dimensions, namely: (1) the subjective experiences of the data subject, (2) the wider regulatory context in which data transparency rights operate, and (3) the socio-technical environment in which they are exercised. Focusing on these three perspectives, we propose a multidimensional framework through which data transparency rights, including their current manifestation within the GDPR, can be both critically reflected upon and further developed.[26]

---

relevance) 2019. Similarly, transparency measures – with potential relevance for data protection – also constitute vital components of recently proposed regulatory initiatives from the EU, such as the Digital Services, Digital Markets and the Artificial Intelligence Acts. The latter frameworks too have been excluded from the scope of our analysis. Proposal for a Regulation of the European Parliament and of the Council of 15 December 2020 on contestable and fair markets in the digital sector (Digital Markets Act) (text with EEA relevance) COM(2020) 842 final; Proposal for a Regulation of the European Parliament and of the Council of 15 December 2020 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (text with EEA relevance) COM(2020) 825 Final; and Proposal for a Regulation of the European Parliament and of the Council of 21 April 2021 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final.

[26] Data protection does not operate within a vacuum and research has recognised that challenges related to data protection are best placed within a broader context, whereby proper account is given to a variety of contexts, perspectives, angles or dimensions. The multidimensional analysis we advance should therefore be positioned within a wider research tradition. For a recent and more concrete example, reference can be made to the work of Hamon, Junklewitz, Malgieri and others. In relation to algorithmic decisions, they propose a multidimensional explanation, whereby the information to be given depends upon factors such as audience, time, granularity and risk. Doing so, they also refer to the work of Kaminski and Malgieri on multilayered explanations. Here, explanations are linked to an algorithmic DPIA process in order to be further contextualised. See Ronan Hamon and others, 'Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 Use Case Scenario', *Proceedings of ACM Facct Conference* (2021 forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3774114 accessed 26 February 2021; Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2020) *International Data Privacy Law* https://doi.org/10.1093/idpl/ipaa020 accessed 26 February 2021. In this regard, the importance of contextual factors has also been explored in the field of transparency and AI, see e.g., the understanding of transparency as a relational concept by Felzmann and others. See Heike Felzmann and

This chapter is structured as follows. First, we outline the importance of data transparency rights in reference to the key functions ascribed to data protection, namely transparency, control and mitigating power asymmetries (Section 2). These functions can also be pursued by data subjects via their data transparency rights, and form an integral part of the first dimension outlined above. Second, we analyse the concrete manifestation of data transparency rights in the GDPR and provide a detailed overview of the relevant provisions (Section 3). The legal framework represents the second dimension within our analysis. Third, we develop the idea that data transparency rights are best viewed as multifaceted instruments and illustrate our findings using the three dimensions outlined above, namely the subjective experiences of the data subject, the legal framework and the socio-technical environment. In doing so, we identify and evaluate the challenges limiting the effectiveness of data transparency rights, while also highlighting their potential (Section 4).

2. GROUNDING DATA TRANSPARENCY RIGHTS: TRANSPARENCY, CONTROL AND POWER

There is no clear consensus on what constitutes the *essence* of the fundamental right to data protection.[27] Still, the right can at least be considered vital in safeguarding values liberal democracies hold dear, from human dignity and autonomy to (informational) self-determination. With that in mind, the right to data protection stemming from Article 8 CFR aims to prevent control over personal data from being curtailed by information-driven power asymmetries.[28] The CFR reveals a highly interrelated and interactive dialogue between the right to data protection and underlying values such as transparency, control and power mitigation. In the following sub-sections, we examine each of these foundational values and look at how

---

others, 'Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns' (2019) 6 *Big Data & Society* 1. On a foundational level, reference can also be made to Bert Jaap-Koops and others' "A Typology of Privacy." They propose a multidimensional model of privacy that is better capable of making visible the multifaceted nature of privacy. See, Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 *University of Pennsylvania Journal of International Law* 483, 570. Similarly, Daniel Solove's understanding of privacy can be seen as a pluralistic and contextual account. See Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477; Daniel J Solove, 'Understanding Privacy' (Social Science Research Network 2008) SSRN Scholarly Paper ID 1127888 https://papers.ssrn.com/abstract=1127888 accessed 26 February 2021.

[27] See generally: Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014); Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2016); Hielke Hijmans, *The European Union as Guardian of Internet Privacy : The Story of Art 16 TFEU* (Springer 2016); Maja Brkan, 'In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy' (2017) Maastricht Working Papers 1/2017 https://papers.ssrn.com/abstract=2900281 accessed 26 February 2021; Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 *Yearbook of European Law*; Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020).

[28] Jef Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (Oxford University Press 2020) 54–90. See also: Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 *International and Comparative Law Quarterly* 569.

they not only ground the data transparency rights contained in the GDPR, but also how they provide a purpose to transparency rights.[29] Being an integral part of data protection, transparency rights as instruments pursue objectives that are inherently linked to the goals underlying the fundamental right to data protection. In Section 4, data transparency rights will be further contextualised through a multidimensional lens in an effort to ascertain to what extent, and under what conditions, transparency and transparency-related goals and objectives can survive the translation from rights-in-theory to rights-in-practice.

2.1 Transparency

The ubiquity of digital infrastructures in modern society requires ever-more expansive data processing. In addition, the current software development paradigm often involves the constant monitoring of users in order to adjust digital services in a continuous feedback-loop.[30] In this context, data transparency rights pursue both an intrinsic and an instrumental goal. First, they should allow individuals to be informed about whether, why and how their personal data are being processed, as well as to know which data are processed, who they have been shared with and for how long they will be stored.[31] In that sense, transparency as an *end* – rather than a *means* – is paramount. Indeed, both the ever-expanding datafication of society and the governance-through-data paradigm, require new forms of transparency in order to make our world and lived experience visible.[32] As such, transparency's intrinsic value in a digital society lies in the fact that it can render artificial environments observable.

Second, data transparency rights are also *instrumental* in enabling other prerogatives. In that sense, 'neither rectification or erasure […] nor blocking or objecting to the processing of personal data seems easy or even possible unless the data subject knows exactly what data [are being processed] and how'.[33] A minimum understanding of the system at stake is therefore necessary before being able to scrutinise and/or challenge its functioning. This also appears from other transparency provisions in the GDPR, such as the need to obtain explicit consent for decision based solely on automated processing within the meaning of Article 22(1) GDPR,[34] to the obligation to notify data subjects in case of a data breach,[35] and the possibility to rely on certification mechanisms.[36]

---

[29] See also Section 4 Data Transparency Rights: A Multidimensional Analysis.

[30] Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Jules Polonetsky, Omer Tene and Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (CUP 2018) https://osf.io/preprints/socarxiv/9gy73/ accessed 26 February 2021.

[31] GDPR, Rec 39.

[32] Mikkel Flyverbom, *The Digital Prism: Transparency and Managed Visibility in a Datafied World* (2019).

[33] See (the many references in): Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4, 7.

[34] GDPR, arts 4(11), 7 *j* 22(2)(c) and Recital 71 GDPR.

[35] GDPR, art 33.

[36] GDPR, art 42.

2.2 Control

Data protection, and by extension data rights, should allow natural persons to 'have control of their own personal data'.[37] This is especially important in light of the political economy of the digital society, where considerations of human wellbeing and self-determination are generally subordinated to the priorities and values of powerful economic actors.[38] Current data-processing eco-systems have become too complex for the legislator to anticipate all potential externalities, and national supervisory authorities often lack the capacity and resources to appropriately tackle non-compliance.[39]

Effective control over one's information is therefore necessary in order for citizens to remain free and autonomous;[40] it introduces friction into the automation of society.[41] Data rights such as the rights of access, to rectification, to erasure, to data portability or to object are easily accessible tools for individuals to understand and control the processing of *their* personal data. That said, strong transparency mechanisms are crucial in order to enable meaningful control. In order to adequately exercise the right to rectification or erasure for example, data subjects will have to be aware of the actual extent of their personal data and how it is being processed. Put differently, data transparency can be considered the 'natural precondition'[42] or 'sine qua non'[43] for data subject empowerment. As also acknowledged by the CJEU, the right of access can pave the way for individuals to exercise control over the way their personal data are pro-

---

[37] GDPR, Rec 7.

[38] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) ch 2.

[39] See: Brave, 'Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities' (April 2020) https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf accessed 28 November 2020; Johnny Ryan, 'Internal problems exposed at Irish Data Protection Commission' (February 2021) https://www.iccl.ie/news/internal-problems-exposed-at-irish-data-protection-commission/ accessed 26 February 2021.

[40] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014).

[41] Cf. Cohen's concept of *semantic discontinuity*, in: Julie Cohen, 'The Networked Self in the Modulated Society' in Wouter De Been, Payal Arora and Mireille Hildebrandt (eds), *Crossroads in New Media, Identity, and Law: The Shape of Diversity to Come* (Palgrave Macmillan 2015).

[42] Xavier Duncan L'Hoiry and Clive Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise Their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 *International Data Privacy Law* 190, 1.

[43] Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8(1) *International Data Privacy Law* 4. On a similar note, Kaminski also sees a strong relationship between the GDPR's individual rights and the need for individualised transparency. In reference to Barocas and Selbst, she argues that the relationship between rights and transparency reveals an interesting component of transparency: 'the substance of other underlying legal rights often determines transparency's substance'. Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 *Berkeley Technology Law Journal* 189, 213; Andrew D Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87 *Fordham Law Review* 1085, 1120–1121.

cessed.[44] In sum, data transparency rights should be seen as critical in empowering (groups of) individuals over data processing activities that affect them.[45]

2.3 Power Mitigation

Data protection can also play a vital role in constraining the accumulation of unprecedented levels of power in the face of rapid technological developments.[46] Digital infrastructures permeate every aspect of our lives, our relationships and our society more broadly. This has enabled the flourishing of highly adaptive and invasive digital choice architectures threatening core values such as autonomy, individual liberty, freedom and informational self-determination. Access and control over (personal) data implies power over (groups of) individuals, especially when combined with the ability to manipulate individuals' environment and lived experiences.[47] The relevant asymmetries are not simply about who has access to the most information, but rather who has the most (actionable) knowledge inferred from that information.[48] The so-called 'datafication of everything' effectively creates measurable types of knowledge which can then be modulated by those in control over the data (often commercial actors), in pursuit of their own interests.[49] Hildebrandt rightfully observed that such asymmetries in power greatly 'challenge the relative autonomy of individual citizens and allow an unprecedented dynamic segmentation of society.'[50]

---

[44] Case C-553/07 *College van burgemeester en wethouders v M.E.E. Rijkeboer* [2009]ECLI:EU:C:2009:293 (Rijkeboer), paras 51–52. See also, on the role of the right of access as an enabler for other prerogatives: Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994 (Nowak), para 57. A similar reasoning may be found in the ECtHR ruling of *Rotaru v Romania*, App no 28341/95 (4 May 2000), para 46, where the Court found that the refusal to grant individuals access to the information stored deprives them of the opportunity to refute it.

[45] Cf. René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020).

[46] GDPR, Rec 6.

[47] See also: William Bogard, 'Welcome to the Society of Control: The Simulation of Surveillance Revisited' in Richard Victor Ericson and Kevin D Haggerty (eds), *The New Politics of Surveillance and Visibility* (University of Toronto Press 2006) 60; Titus Stahl, 'Indiscriminate Mass Surveillance and the Public Sphere' (2016) 18 *Ethics and Information Technology* 33, 33, 35–36; Angelina Fisher and Thomas Streinz, 'Confronting Data Inequality' (2021) IILJ Working Paper 2021/1 https://www.iilj.org/wp-content/uploads/2021/04/Fisher-Streinz-Confronting-Data-Inequality-IILJ-Working-Paper-2021_1.pdf accessed 25 June 2021; Marijn Sax, 'Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps' (2021) (PhD thesis)

[48] Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (First, IOS Press 2012) 49 https://works.bepress.com/mireille_hildebrandt/40/ accessed 26 February 2021.

[49] Antoinette Rouvroy, 'The End(s) of Critique: Data-Behaviourism vs. Due-Process' in Mireille Hildebrandt and Katja de Vries, *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2013); Antoinette Rouvroy, '"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data' (2016) T-PD-BUR(2015)09REV https://rm.coe.int/16806a6020 accessed 21 February 2021; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (First, IOS Press 2012); John Cheney-Lippold, *We Are Data: Algorithms and the Making of Our Digital Selves* (New York University Press 2017) ch 2: Control.

[50] Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (First, IOS Press 2012), 54.

Data rights appear to be well suited to resist and break down such emerging shifts in power. Indeed, combined with legal restrictions and obligations directed at the architects of today's digital infrastructures, data rights have the potential to constrain power asymmetries and the ensuing externalities to fundamental rights, freedoms and interests. They do so by straightjacketing those controlling our data and our digital behaviour. Both by requiring the implementation of specific compliance mechanisms to accommodate data rights, as well as the ability for individuals to proactively control how their data is being processed. The right of access allows data subjects to verify and monitor controllers' compliance with the GDPR. Should irregularities be discovered this way, obtained insights can then serve as a starting point for remedial action.[51] This is also reflected in Recital 63 GDPR which suggests that the right of access be used 'to verify the lawfulness of the processing'. Likewise, scholars have shed light on the collective dimension of the right of access to challenge all kinds of externalities produced by powerful actors.[52] Data transparency rights may thus play a crucial role in countering information asymmetries, and as such, act as a first step in opposing data-driven power asymmetries.

3. DATA TRANSPARENCY RIGHTS: THE LEGAL FRAMEWORK

The GDPR lays down rules to guarantee the respect of individuals' fundamental rights – including but not limited to data protection – in situations involving the processing of their personal data.[53] It has established a system of checks and balances which strives to achieve a fair balance between all competing rights, freedoms and interests as they are affected by the processing of one's personal data.[54] Among many other things, the GDPR substantiates fairness and empowerment as dimensions that shall be protected through extensive transparency requirements within an increasingly complex digital society. Combined with clearer and more extensive modalities, (groups of) individuals are now better equipped to understand and control the use of their personal data. In the GDPR, the aforementioned facets of data protec-

---

[51] Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8(1) *International Data Privacy Law* 5. See also, on the link between the right of access and the right to an (effective) remedy for data protection violations: Antonella Galetta and Paul De Hert, 'The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?' (2015) 8 *Review of European Administrative Law* 125.

[52] René L P Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 *Internet Policy Review* 3; René Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' (LawArXiv 2020) preprint https://osf.io/b5dwm accessed 7 July 2020; René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020).

[53] While art 1(2) GDPR puts the emphasis on 'the protection of personal data', Rec.4 GDPR clarifies that the rules stemming from the Regulation respects "all fundamental rights" and observes "the freedom and principles recognised in the Charter".

[54] See, on the scope, interpretation and relationship of art 8 CFR with other fundamental rights: Steve Peers and others, *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 223–266.

tion are reflected in some of the general principles governing the processing of personal data, the controller's ex-ante transparency obligations, the data subject's ex-post right of access and the possibility to request more information in case of automated decision-making (hereinafter ADM) processes.

In this section we provide an overview of the transparency tools at data subjects' disposal, and Articles 12, 13, 14, 15 and 22 GDPR in particular. As will appear later, the *actual* role data transparency rights ultimately hold will follow from a multidimensional calculus. More specifically, the value of transparency rights depends on the interaction between the relevant legal framework, the wants and needs of the data subject, and the socio-technical environment through which data subjects navigate.

3.1 Of Fairness, Lawfulness and Transparency

Article 5 GDPR details the general principles governing the processing of personal data. Of critical importance when it comes to complex processing operations – and especially decisions based solely on automated processing – are the principles of lawfulness, fairness and transparency, now all bundled under Article 5(1)a GDPR.

On the one hand, fairness within the meaning of the GDPR is a versatile concept that often goes hand in hand with transparency, the latter frequently being considered a precondition of the former.[55] For data processing operations to be fair, controllers must adequately consider the reasonable expectations of the data subjects as well as potentially adverse consequences stemming from the processing.[56] Fairness plays an implicit role in protecting data subjects involved in asymmetric relationships via the various balancing exercises embedded in data protection law. More importantly, fairness is also the prism through which compliance with transparency requirements is to be assessed, and serves as a guiding principle for controllers when accommodating data subjects' rights. Transparency, on the other hand, percolates through the entire text of the Regulation and requires controllers to inform data subjects that 'personal data concerning them are collected, used, consulted or otherwise processed, and to what extent the personal data are or will be processed'.[57]

Transparency is closely linked to lawfulness since proper information is a prerequisite for the lawful grounds listed in Article 6(1) GDPR. Consent, for instance, is only valid if it is given after data subjects have been provided with the information necessary to understand what they are agreeing to.[58] Likewise, controllers relying on a contract to justify their process-

---

[55] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Y*earbook of European Law* 130 138–140; European Union Agency for Fundamental Rights and others (eds), *Handbook on European Data Protection Law* (Office of the European Union 2014) 75–78. See also, Case C-201/14 *Bara* [2015] ECLI:EU:C:2015:638, paras 34 sqq.

[56] Article 29 Working Party, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed 26 February 2021, para 12.

[57] GDPR, Rec 39.

[58] Article 29 Working Party, 'Guidelines 05/2020 on consent under Regulation 2016/679' 4 May 2020 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf accessed 26 February 2021, para 62.

ing operations should 'avoid any confusion' as to the applicable lawful ground[59] and clearly circumscribe the purposes for which the processing takes place, so as to verify that it is indeed 'objectively necessary' for the performance of the contract.[60] The same is true for the legitimate interest ground, in which case controllers should document their 'balancing of interests' in a sufficiently detailed manner so as to allow verification by the relevant stakeholders.[61]

Transparency is also an important consideration for controllers who are not only required to ensure, but also to demonstrate, compliance throughout the entire data processing life cycle.[62] This is materialised, for instance, by the obligation to keep a record of their processing activities.[63] Here, transparency becomes an instrument of accountability that allows public and regulatory scrutiny, and enables the relevant stakeholders to assess and, if necessary, challenge certain processing operations. For example, transparency allows data subjects to better assess how to exercise their rights under the GDPR against a given controller, ranging from a withdrawal of consent (art 7(4)), to access (art 15) or portability (art 20) requests.[64] Transparency offers data subjects insight into the existence and the scope of the processing activities, and against whom and how to practically exercise their rights.

As a guiding principle, transparency is further solidified by Article 12 requiring that any information referred to in Articles 13 and 14, and any communication under Articles 15–22 GDPR relating to processing must be given to the data subject in a concise, transparent, intelligible and easily accessible form, using clear, and plain language.[65] Transparency manifests itself in multiple ways throughout the GDPR. It can take the form of both (i) ex-ante and

---

[59] Article 29 Working Party, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed 26 February 2021, para 20.

[60] Article 29 Working Party, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed 26 February 2021, para 24.

[61] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' 9 April 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf accessed 26 February 2021, 43. The Working Party (pp 43–44) has recommended for controllers to 'explain to data subjects in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects" and detail "the safeguards they have taken to protect personal data'.

[62] See e.g., GDPR, arts 5(2); 24(1) and 25(1); Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 2.

[63] See GDPR, art 30.

[64] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 2. See also Case C-201/14 *Bara* [2015] ECLI:EU:C:2015:638, para 33 and the Opinion of AG Cruz Villalón, para 74:

> the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed […] and their right to object to the processing of those data.

[65] GDPR, Rec 39 and art 12 (1). See also infra, Sections 3.2, 3.3 and 3.4. It could be further explored to what extent controllers should alter their communication to the data subject depending on the right in question; e.g., should the way a data controller communicates to the data subject under a right of access

ex-post measures, depending on whether information is given before or after the processing; and (ii) through empowerment or protective mechanisms, depending on whether access to information requires a proactive attitude from the data subject or not. While all transparency provisions ultimately serve to strengthen the overall position of the data subject, measures can be considered as more empowering when they directly provide individuals with the tools to control their data at the data subject's initiative. Protective measures primarily place the burden on controller to make sure that the relevant information is made available to data subjects in a concise and intelligible way.

3.2 Articles 13 and 14 GDPR: The Ex-Ante Transparency Requirements

From an ex-ante and protective perspective, transparency is mainly given shape by Articles 13 and 14 GDPR, which enumerates the information controllers must provide data subjects up front, and on the controllers' own initiative. Article 13 GDPR applies where personal data are collected directly from the data subject, whether through observation or through data subjects actively providing said data.[66] Article 14 GDPR deals with the situation where personal data have not been obtained from the data subject. In the latter case, the controller has obtained data from others, such as third parties, publicly available sources, data brokers or even other data subjects.[67]

The two provisions can further be distinguished based on timing, scope and actual transparency requirements. As to timing, Article 13(1) GDPR requires controllers to provide the necessary information 'at the time when personal data are obtained'. In case of data not obtained directly from the data subject, Article 14(3) GDPR states that the said information must be made available 'within a reasonable period after [the controller] obtained the personal data', 'at the time of the first communication with the data subject' or 'when the personal data is first disclosed', but in any case 'no later than one month' after the data have been obtained.[68] Content-wise, there is not much difference between Articles 13 and 14 GDPR beyond the inclusion of the categories and sources of personal data in Article 14 GDPR (see Table 21.1).[69] As far as limitations are concerned, Article 13(4) GDPR exempts controllers from providing

request differ from the way they communicate under a request to erasure? Unfortunately, such an investigation into the various 'right-dependent modes of communication' falls outside the scope of this chapter.

[66] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 26.

[67] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 26. In addition, it follows from the 'such as' that this list was not meant by the Article 29 Working Party as exhaustive.

[68] As highlighted by the Article 29 Working Party, the wording of art 14(3)b and c suggests that the general one-month time limit of art 14(3)a remains applicable regardless of the circumstances detailed in b and c. Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 27.

[69] The Article 29 Working Party has also clarified that no distinction should be made between the information listed in paragraphs 1 and 2 of arts 13 and 14 GDPR. See: Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 23.

that information 'insofar as the data subject already has that information', while Article 14(5) GDPR extends that exemption to cases where 'the provision of such information would prove impossible or involve a disproportionate effort' and where the data 'must remain confidential subject to an obligation of professional secrecy'.

Ex-ante transparency requirements play a critical role regardless of the complexity of the processing operations. They allow data subjects to grasp the extent and purposes of the processing operations by providing information on, for example, the purpose(s) and lawful ground(s). They also ensure that data subjects are provided with the necessary information for exercising their rights, such as the availability and scope of specific rights,[70] and the contact details of the controller, in case they wish to pursue remedial actions. Recital 39 GDPR, although not legally binding, complements the list of information to be provided to data subjects with the 'risks, rules, safeguards and rights in relation to the processing of personal data', the outcome of an assessment typically conducted in the context of a Data Protection Impact Assessment.[71] This reinforces the idea that, beyond the strict provision of specific information to data subjects, transparency as a general data protection principle requires controllers to set up and maintain data hygiene throughout the entire data processing life cycle.

The form of information requirements is equally important as its content. Article 12 GDPR details the modalities according to which the information referred to in Articles 13 and 14 must be made available to data subjects. Controllers should provide information in a 'concise, transparent, intelligible and easily accessible way',[72] which requires controllers to communicate in such a way as to avoid information fatigue.[73] Intelligibility is crucial for complex processing operations, since it requires controllers to tailor the way they present the necessary information to their audience.[74] The latter presupposes awareness of the type of users whose data will be

---

[70] Cf. Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International Data Privacy Law* 4, 15–16.

[71] See: European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf accessed 26 February 2021, para. 30; European Data Protection Supervisor, 'Opinion 5/2018 – Preliminary Opinion on privacy by design', 31 May 2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf accessed 29 June 2021, para. 40; Dariusz Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process' https://researchportal.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developin accessed 29 June 2021, 53; Laurens Sion and others, 'An Architectural View for Data Protection by Design', *Proceedings of the 2019 International Conference on Software Architecture* (IEEE 2019) 1.

[72] GDPR, art 12(1).

[73] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 202, para 8.

[74] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 9. This idea also transpires from Rec 58 GDPR:

> This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.

Table 21.1 Information to be provided under Articles 13, 14 (ex-ante) and 15 (ex-post) GDPR

Information to be provided to data subjects			
Recommended information	**Relevant recitals**		
Risks, rules, safeguards and rights in relation to the processing of personal data and how data subjects can **exercise** their **rights** in relation to such processing.	39		
Where the **origin** of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.	61		
In the context of ADM within the meaning of Article 22 GDPR, **specific information** to the data subject and the right to obtain human intervention, to express their point of view, **to obtain an explanation of the decision reached** after such assessment and to challenge the decision	71		
	Relevant articles		
Required information	Art. 13 (Rec. 60, 61, 62)	Art. 14 (Rec. 60, 61, 62)	Art. 15 (Rec. 63, 64)
Confirmation as to whether or not personal data are processed	-	-	(1)
Copy of the personal data being processed	-	-	(1)(3)
Identity and **contact details of the controller** and, where applicable, its **representative**	(1)a	(1)a	-
Contact details of the data protection officer, where applicable	(1)b	(1)b	-
Purposes of the processing	(1)c	(1)c	(1)a
Legal basis for the processing	(1)c	(1)c	-
Categories of personal data concerned	-	(1)d	(1)b
Where the processing is based on point (f) of Article 6(1), **legitimate interests pursued** by the controller or by a third party	(1)d	(2)b	-
Recipients or categories of recipients of the personal data, if any	(1)e	(1)e	(1)c
Details on potential **data transfers to third countries**	(1)f	(1)f	(2)
Retention period, or if that is not possible, the **criteria** used to determine that period	(2)a	(2)a	(1)d
Existenceof the **right to access**	(2)b	(2)c	-
Existence of the **right to rectification**	(2)b	(2)c	(1)e
Existence of the **right to erasure**	(2)b	(2)c	(1)e
Existence of the **right to restriction of processing**	(2)b	(2)c	(1)e
Existence of the **right to object to processing**	(2)b	(2)c	(1)e
Existence of the **right to data portability**	(2)b	(2)c	-
Where the processing is based on consent, the existence of the **right to withdraw consent** at any time	(2)c	(2)d	-
Right to lodge a complaint with a supervisory authority	(2)d	(2)e	(1)f
Whether the provision of personal data is a statutory or contractual **requirement**, or a requirement necessary to enter into a contract, as well as **whether the data subject is obliged to provide the personal data** and of the possible **consequences of failure** to provide such data	(2)e	-	-
Source from which the personal data originate, and if applicable, whether it came from publicly accessible sources [a]	-	(2)f	(1)g
Existence of ADM, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information about the logic involved**, as well as the **significance and the envisaged consequences** of such processing for the data subject.	(2)f	(2)g	(1)h

processed and requires adapting the tone and language to the targeted group.[75] Finally, the 'easily accessible' condition requires controllers to be proactive: data subjects should not look for the information, but instead, it should 'be immediately apparent to them where and how this information can be accessed'.[76]

Information should be presented in 'clear and plain language, in particular for any information addressed specifically to a child'.[77] Controllers should refrain from relying on complex sentences and language structures, but provide concrete and definitive information that is 'not phrased in abstract or ambivalent terms or leave room for different interpretations'.[78] 'Language qualifiers such as "may", "might", "some", "often" and "possible" should be avoided, as well as the use of "overly legalistic, technical or specialist language or terminology".'[79] As hinted above, transparency is a context-dependent moving target. As a result, providers of particularly complex technologies, or those targeting less-literate groups, will need to put in the effort for their audience, and most notably, describe unambiguously the most important anticipated consequences the data operations hold for those involved.[80] The information provided must match the actual processing activities of the controller and can be accompanied by standardised icons.[81]

Finally, Article 12(1) GDPR states that the information can be provided in writing 'or by other means, including, where appropriate, by electronic means'. When it comes to written electronic means, a layered approach has been recommended, be it in a digital or non-digital context, to 'allow website visitors to navigate particular aspects of the privacy notice that are of most interest to them'.[82] Such an approach can be a way to reconcile the requirements of

---

[75] In the presentation of information, the use of nudges and deceptive techniques to provide the information and orient data subjects' choice is at odds with the principle of fairness and data protection by default.

[76] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 11. This, adds the Article 29 Working Party, can be achieved by providing the information directly to data subjects, linking them to it, signposting it or, by giving the information as an answer to a natural language question, for example in the form of an FAQ.

[77] GDPR, art 12(1).

[78] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 12.

[79] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para. 13.

[80] See: Priya Kumar, 'Privacy Policies and Their Lack of Clear Disclosure Regarding the Life Cycle of User Information', *2016 AAAI Fall Symposium Series* (2016); Tsai-Wei Chen and S Shyam Sundar, 'This App Would Like to Use Your Current Location to Better Serve You: Importance of User Assent and System Transparency in Personalized Mobile Services', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018) http://doi.acm.org/10.1145/3173574.3174111 accessed 17 May 2018. This is also evidenced by the development of platforms and tools to streamline the reading of privacy policies such as: Terms of Service; Didn't Read https://tosdr.org/ accessed 26 February 2021.

[81] No such standardised icons have been proposed yet. It is for the European Commission 'to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedure for providing standardised icons' (art 12(8) GDPR).

[82] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26

conciseness and completeness. All in all, it is crucial that the method chosen to provide the information is appropriate to the specific scenario. For example, providing the information only in writing might prove inappropriate for a screenless device, such as a smart-speaker.[83]

3.3 Article 15 GDPR: The Ex-Post Right of Access

From an ex-post empowerment perspective, Article 15 GDPR complements the ex-ante transparency requirements laid down in Articles 13 and 14 GDPR by granting data subjects the right to request (1) confirmation that personal data concerning them are being processed, (2) individualised details on the relevant processing operations and (3) a copy of the personal data involved (see Table 21.1 above). Not only does this prerogative play a pivotal role in the GDPR (see *infra*), but it is also regarded as an integral part of the fundamental rights to privacy and data protection guaranteed by both the ECHR[84] and the CFR.[85]

The right of access allows data subjects to go beyond what is provided in a data policy and request more information on how their personal data is processed, therefore offering an additional, individualised layer of transparency. The overlap between the elements listed in Articles 13 and 14 GDPR and the ones included in Article 15 (see Table 21.1) suggests that the details communicated by controllers in the latter case should be more granular and, to the extent possible, tailored to the specific situation of the data subject exercising their right.[86] Controllers should therefore not answer a request for access by repeating the generic information that is already available in the data policy, but provide details pertaining to the data subject's specific situation. This implies, for instance, listing the actual recipients with whom specific personal data have been shared or the logic behind a particular ADM. Exercising the right of access could thus facilitate the understanding of complex processing operations, the inner functioning of which might be too dense to fit in a regular data policy or which significantly varies from one data subject to another.

February 2021, para 17; 35.

[83] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 19.

[84] The Strasbourg Court has already stressed that denying or ignoring an access request, whether in the case of information held by public authorities or private actors, could amount to a disproportionate interference under art 8(2) of the ECHR if that decision failed to strike a fair balance between competing interests See among others: ECtHR, *Leander v Sweden*, 26th March 1987; *Gaskin v the United Kingdom*, 7 July 1989; *Z. v Finland*, 25th February 1997; *M.G. v the United Kingdom*, 24th December 2002; *Odièvre v France*, 13th February 2003; *I. v Finland*, 17 July 2008; *Haralambie v Romania*, 27th October 2009.

[85] Article 8(2) CFR explicitly states that 'Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.' This chapter was finalised before the publication of the European Data Protection Board's guidelines on the right of access, which were adopted and announced in January 2022. See: European Data Protection Board, 'EDPB Adopts Guidelines on Right of Access and Letter on Cookie Consent' (19 January 2022); <https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-right-access-and-letter-cookie-consent_en> accessed 21 January 2022.

[86] Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 462; Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC 293.

The right of access is only one piece of the fairness puzzle however, the focal point of which lies in the expectations of data subjects. While ex-ante transparency may shape those expectations, the right of access allows them to dig deeper and verify the extent of controllers' data processing practices (and take remedial action if need be).[87]

Similar to the ex-ante transparency obligations, any communication with the data subject following an access request must be formulated in a concise and intelligible manner using clear and plain language, with proper attention for the modalities through which access can be provided.[88] Article 12(2) GDPR also obliges controllers to facilitate the exercise of data subjects' rights – including but not limited to access – by, for instance, setting-up different modalities for access depending on the ways in which data subjects interact with the controller.[89] As a result, Recital 59 GDPR adds that it should be possible for the data subject to file the request electronically, in which case the answer should also be provided by electronic means unless otherwise requested by the data subject.[90] Besides, there is no predefined means or format governing the sending of access request, which could even be sent via social media and with no reference to the text of the GDPR or its provisions.[91]

The controller cannot refuse access merely because the request is complex.[92] It can nonetheless 'request the subject to specify the information or processing activities to which the request relates'.[93] Once again, a heavier burden is placed on controllers that engage in complex pro-

---

[87] GDPR, arts 16–22, 77, and 82. See in this regard also the Uber and Ola cases referenced under (n 2), and further observations made regarding these rulings under (n 34, 111, 117 and 161). The Amsterdam District Court's rulings provide a concrete example concerning the practical, complementary and empowering role access rights can have within the digital society, both in relation to general data processing operations and solely automated decision-making procedures.

[88] See GDPR, art 12, and Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 55.

[89] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021, para 55.

[90] GDPR, art 12(3).

[91] Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 465. The author refers to the guidance on the right of access available on the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ accessed 26 February 2021.

[92] Only where a request is manifestly unfounded or excessive, and in particular because of its repetitive character, could the controller charge a fee or refuse to act; GDPR, art 12(5).

[93] GDPR, Rec 63. On this particular point, the Amsterdam District Court (n 2 and 87) reiterated that where access to data had already been provided in the past, data subjects may be required to further specify to which information or processing activities their request relates. As such, an access request pertaining to all information processed may be considered too general, and can therefore be rejected for being too insufficiently defined. In reaching this concluson, the Court referred to Rec 63 GDPR: 'Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.' See also Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019 accessed 23 June 2021, para 4.17; Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1020 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020 accessed 23 June 2021, para 4.35.

cessing operations since they will have to ensure that the information shared with data subjects following an access request is sufficiently clear and intelligible.[94] In the same vein, the data subject does not have to justify their request, which could be filed for a wide variety of reasons ranging from mere transparency to investigative journalism.

Finally, the GDPR introduced clear time limits for the handling of data subject's requests. Controllers must now provide "information on action taken […] without undue delay and in any event within one month of receipt of the request"; a period that can only be extended by another two months under strict conditions.[95] Article 12(3)'s wording can be interpreted as only installing time constraints for informing data subjects about the progress made by a controller to address an access request, without providing a substantive answer.[96] In other words, while controllers are required to inform the data subject after one month, complexity can buy them time to accommodate more difficult requests.

3.4 Automated Decision-making: Increased Transparency?

Over the last few years, there has been a growing realisation as to the need to ensure appropriate transparency and accountability for increasingly complex decision-making systems, especially where human involvement is limited or non-existent. In this context, a number of GDPR provisions have fuelled a lively debate among scholars as to the existence of a so-called 'right to an explanation' of ADM.[97] While this section does not intend to offer a full-fledged overview of all arguments raised, it nonetheless aims at clarifying the key provisions around which the transparency in ADM debate revolves.[98]

---

[94] As such, complexity is not an excuse to escape their responsibilities, but rather a reason to put even more effort when accommodating data subject's rights. See: Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC 286, para 20.

[95] GDPR, art 12(3).

[96] See also, of the same opinion: Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 465.

[97] Contributors include *among others*: Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 *AI Magazine* http://arxiv.org/abs/1606.08813; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 243. Margot E Kaminski and Gianclaudio Malgieri, 'Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020) https://doi.org/10.1145/3351095.3372875 accessed 5 May 2020. Ronan Hamon and others, 'Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 Use Case Scenario.', *Proceedings of ACM Facct Conference* (2021 forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3774114 accessed 26 February 2021. Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 *Berkeley Technology Law Journal* 189.

[98] It should be noted the GDPR is not the first regulatory framework to introduce specific transparency obligations vis-à-vis automated processing. Back in 1978, the first French data protection act, for instance, already granted data subjects a 'right to know' and to 'challenge the logic used by automated processing whose results are opposed to them'. See: Loi n°78-17 du 6 janvier 1978 relative à l'infor-

At first sight, the GDPR appears sensitive to the particular dangers posed by ADM. Articles 13(2)f, 14(2)g and 15(1)h GDPR lay down additional informational guarantees where ADM are deployed. However, before analysing their actual content, it should be noted that aforementioned ADM-related transparency provisions do not refer to ADM in general, but to the types of ADM referred to under Article 22 GDPR.[99] Given the pivotal role ascribed to Article 22 GDPR, we must first understand what this particular provision entails.

Article 22 GDPR grants data subjects the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning him or her or similarly significantly affects him or her. In this regard, any reference to Article 22 implies that additional informational benefits apply only to a) *decisions* that b) are *based solely*[100] on automated processing or profiling,[101] and c) that produce *legal effects* or similarly *significantly affect* data subjects.[102] In the absence of any binding definition, the concept of 'decision' could arguably be interpreted broadly as 'a particular attitude or stance' that has a sufficient degree of 'binding effect' so as to be 'acted upon'.[103] Still, it is unclear whether this would only cover a decision that has a concrete outcome for the data subject (the denial of a bank loan) or also the intermediary decisional steps leading to the said outcome (the creation of the profile used to refuse said loan). The notion 'based solely' suggest that the decision is reached without any (meaningful) human intervention or involvement. A 'legal effect' entails an effect on one's legal rights, status or rights under a contract.[104] What it means for a decision to 'similarly significantly' affect the data subject is more difficult to grasp. While Recital 71 GDPR high-

---

matique, aux fichiers et aux libertés, initial version available here https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460 accessed 21 February 2021, quoted by Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 463.

[99] These provisions require the data subject to be informed regarding 'automated decision-making, including profiling, referred to in Article 22(1) and (4)'. See, GDPR, arts 13(2)f, 14(2)g and 15(1)h.

[100] The word 'based' suggests that the decision must not necessarily be 'taken' solely by an automated system. The routine application of automatically generated information by a person not in a position to exercise any influence or meaningful oversight on the outcome would also fall under art 22(1) GDPR. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 20–21.

[101] The wording of art 22(1) GDPR – i.e., 'decision based solely on automated processing, including profiling', allows for two interpretations. Either 'profiling' is on equal footing with 'automated processing', and therefore an alternative criteria determining the scope of application of art 22(1); or 'profiling' is regarded as an additional condition narrowing down the scope of 'automated processing'. As highlighted by Bygrave, the use of a comma to separate both terms suggests that the decision can either be based on automated processing or on profiling (Lee A Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 530). The Article 29 Working Party also seems to share that view (Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 8).

[102] For more thorough discussions regarding these conditions, see also the literature under (n 97).

[103] Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law* (Springer International Publishing 2017) http://link.springer.com/10.1007/978-3-319-64955-9_4 accessed 1 October 2020.

[104] For example, an automated decision process that is used to allocate or deny a social welfare benefit under the law, produces a legal effect. See Article 29 Working Party, 'Guidelines on Automated individ-

lights the 'automatic refusal of an online credit applications' or 'e-recruiting practices without any human intervention' as examples, the notion seems broader. The addition of 'similarly' suggests that the threshold for significance must be similar to that of a decision producing legal effect,[105] whereas a 'significant effect' must seemingly have the potential to affect 'the circumstances, behaviour or choices of the individuals', 'have a prolonged or permanent impact on the data subject' or 'at its most extreme, lead to the exclusion or discrimination of individuals'.[106] While clarifications are expected through the interpretation and enforcement by national supervisory authorities, the contours of Article 22 GDPR remain blurry.

That being said, if the conditions of Article 22(1) GDPR do apply, what information must be provided? First, Articles 13(2)f and 14(2)g GDPR require controllers to inform data subjects about the existence of ADM and to provide meaningful information about the logic involved and the significance and envisaged consequences of the processing. Article 15(1)h GDPR mirrors the above-mentioned provisions and grants data subjects the right to obtain (confirmation of) the same information in the context of a subject-specific access request. As mentioned earlier, the controller is under the obligation to communicate in a concise, intelligible and easily accessible form, using clear and plain language.[107]

When providing 'meaningful information as to the logic involved', controllers are advised to avoid 'complex mathematical explanations' about the functioning of the algorithm or machine-learning technique deployed and to rather focus on concrete elements such as:

> the categories of data that have been or will be used in the profiling or decision-making process; why these categories are considered pertinent; how any profile used in the ADM process is built, including any statistics used in the analysis; why this profile is relevant to the ADM process; or how it is used for a decision concerning the data subject.[108]

---

ual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 21.

[105] Such a link between the 'legal effects' and other 'significant effects' was not included in art 15 of the Directive 95/46, the predecessor of art 22 GDPR. See: Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 21 and Lee A Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) 534.

[106] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 21, which lists the following examples:

> decisions that affect someone's financial circumstances, such as their eligibility to credit; decisions that affect someone's access to health services; decisions that deny someone an employment opportunity or put them at a serious disadvantage; decisions that affect someone's access to education, for example university admissions.

[107] GDPR, art 12(1).

[108] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 31. Importantly, the duty to provide comprehensible information ought not to be used as a defence to refuse to provide more detailed/technical information upon request. See: Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC 288 et seq.

The data subject should also obtain meaningful information regarding the significance and envisaged consequences of the processing, which relates to the intended use of the automated process by the controller, and its impact for the data subject. Here, controllers are encouraged to give concrete examples rather than statistics.[109] The future-oriented nature of the word 'envisaged' used in Articles 13(2)f and 14(2)g, as well as Article 15(1)h, seemingly suggests that controllers are not obliged to provide an explanation of a particular decision. However, said information should in principle have already been given to the data subjects in line with the ex-ante transparency obligations. As such, 'the controller should provide the data subject with the information about the *envisaged consequences* of the processing rather than an explanation of a *particular* decision'.[110] As a consequence then, it would appear that these provisions do not introduce any distinction between the information provided ex-ante and ex-post. This would be strange however, as it seems at odds with the role of ex-post empowerment mechanisms which should allow the data subject to obtain more information about their specific situation.[111]

In addition, Article 22 GDPR too introduces transparency safeguards. Article 22(3) GDPR requires controllers to implement suitable measures to safeguard data subjects' rights including, at least, the right to obtain human intervention, to express their point of view and to contest the decision.[112] Recital 71 GDPR adds to that list the controversial 'right' to 'obtain an

---

[109] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 26. See also, on that specific point: Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences' [2018] CoRR http://arxiv.org/abs/1706.07269 accessed 8 September 2020.

[110] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 27.

[111] See Gabriela Zanfir-Fortuna, 'Article 15. Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation - A Commentary* (Oxford University Press 2020) and Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC. See also the Amsterdam District Court's rulings (n 2, 93, 87 and 117). These cases were among the first to provide insight as to how national courts could deal with the interpretation of automated decision-making systems under art 22 GDPR. In the case against Ola, the Court concluded that data subjects were provided insufficient information regarding the system's allocation of penalties and deductions. The latter decision-making process had to be considered a solely automated decision-making process with a similar significant effect covered by arts 15(1)h and 22 GDPR. The Court ordered Ola to provide the requesting parties information that would allow them to understand and verify the choices, data and assumptions underlying the automated decision. The access request also extends to the most significant evaluation criteria used, including their function in relation to the automated decision. Following the request, data subjects must understand which criteria lie at the basis of a decision and they should be able to verify whether the processing of their data was lawful and correct. Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019 accessed 23 June 2021, paras 4.41, 4.51 and 4.52.

[112] The term 'right' 'does not mean that Article 22(1) applies only when actively invoked by the data subject'. Rather, 'Article 22(1) establishes a general prohibition for decision-making based solely on automated processing' which 'applies whether or not the data subject takes an action regarding the processing of their personal data'. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 19.

explanation of the decision reached', often deemed a *sine qua non* in order to meaningfully accommodate the safeguards mentioned in Article 22(3) GDPR. In this context, questions have also been raised whether Article 15(1)h GDPR – compared to its *ex ante* counterparts Articles 13(2)g and 14(2)f – provides data subject the right to request information about how a *specific* decision was reached, rather than a mere explanation of the functioning of the automated system.[113] While the provision of general information such as the 'factors taken into account' and their 'respective weight on an aggregated level' seems sufficient,[114] it nonetheless appears complicated for data subjects to meaningfully exercise their rights if they are not aware of the actual reasoning behind the contested decision.[115] This holds true for both the specific safeguards mentioned in Article 22(3) and Recital 71 GDPR, and for the more traditional prerogatives such as rectification or erasure.

A combined reading of Articles 13(2)g, 14(2)f, 15(1)h, 22(1) and (4) suggests that, while a heightened level of transparency is encouraged for ADM processes that fall outside the scope of Article 22, there is no general obligation to actually do so.[116] Regardless of the above-mentioned controversies and of whether a specific processing falls within the scope of Article 22(1) GDPR however, one must keep in mind that any kind of processing on personal data, including general ADM processes, remains subject to the overarching principles of fairness, lawfulness, transparency and accountability, which require controllers to implement the necessary measures to inform and empower data subjects, and be able to demonstrate that they did so. With this in mind, it remains a good practice to provide the information listed in articles 13(2)f, 14(2)g and 15(1)h) GDPR.[117]

---

[113] See in this regard also the literature mentioned in (n 97).

[114] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 26–27.

[115] Contesting a decision might prove difficult for data subjects if they do not know exactly which factors have been taken into account in their particular case, and therefore which part of the decision-making process to contest. Similarly, their perspective is likely to be limited to expressing their disagreement with the outcome of the decision if they are not given any substance as to how said decision was reached. Likewise, human involvement is of little help in case it leads to a blanket confirmation of the automated decision adopted earlier, especially if no further justification is given as to the reason why the decision has (or has not) been confirmed. See also observations made under (n 111).

[116] See on this point also Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 243, 250.

[117] See also: Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' 6 February 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 26 February 2021, 25. While increased transparency should *a priori* be encouraged, it must be noted that the application of the GDPR's general transparency requirements could already facilitate and advance data subjects' empowerment. As an example of the latter, reference can again be made to the Amsterdam District Court's rulings on the transparency of gig-driver platforms, mentioned at (n 2, 87, 93 and 111). For example, in the case against Ola, the Court had to consider whether the earning profile assigned to drivers constituted an automated decision in the sense of art 22 GDPR. The driver's 'earning profile' comprised a combination of parameters, such as turnover, attendance, hours logged and the driver's score. The profile could be used by Ola to award certain drivers a bonus. According to the Court, the impact of bonus allocations did not appear to create a legal effect or a similarly significant effect. Therefore the profile did not constitute a decision understood by art 22 GDPR. Still, the Court did point out that the earning profile nonetheless remained a case of (personal data) profiling under art 4(4) GDPR as the data were used to evaluate the professional

4. DATA TRANSPARENCY RIGHTS: A MULTIDIMENSIONAL ANALYSIS

Having discussed the values underlying the data transparency rights, and their manifestations within the GDPR, we now take a step back and look at several dimensions that may not only affect the overall effectiveness of data transparency rights, but may also inform their further development. To this end, we distinguish (at least) three broad dimensions:

(1) The data subject dimension (the data subject's subjective experiences);
(2) The legal dimension (the wider regulatory context in which data transparency rights operate); and
(3) The socio-technical dimension (the environment in which data transparency rights operate, and in particular, the actors and technologies, including their interrelations, the data subject interacts with).

For our purposes here, it is useful to consider each of these dimensions sequentially. First, the data subject is confronted with the manifestation of the controller's transparency requirements, be it in the form of design cues and contextual information provided through the interface of the service itself, or in the form of a more traditional data policy. Should that information be incomplete or insufficient, the data subject will be able to leverage the GDPR's regulatory framework to have the controller clarify or complete the missing pieces. Whether that information ultimately proves satisfactory will partially depend on the motivations of the data subject, and the underlying goals for which information was sought. Second, the legal interpretation of the GDPR further influences the effectiveness of data transparency rights. Of course, that perceived efficiency might again depend on the specific situation and expectations of the data subject. Third, the ways data transparency rights are exercised, operationalised and perceived does not solely depend on the data subject, nor the respective legal framework, but also upon the broader socio-technical environment in which they are exercised. This refers, *among others*, to data subjects' interactions with other relevant data actors and the technological systems they rely on.

This section highlights the key challenges that arise within each dimension and that could (potentially) interfere with the values ascribed to data transparency rights. While the GDPR provides a baseline value, data rights can be either 'up-' or 'downgraded' depending on the wants and needs of the data subject, as well as the socio-technical environment in which they are exercised.

---

performance of drivers. The Court thus concluded that Ola should have provided insight into the personal data that were used to generate the profile. Likewise, drivers should have received information regarding the segments in which they were categorised. The latter would have allowed the drivers to verify whether said information was correct. For this, the Court relied upon art 15 GDPR, which grants data subjects the right to obtain access to the data used for profiling purposes, and the categories of data used to create the profile. The Court came to a similar conclusion with regard to Ola's fraud probability score. The aforementioned considerations illustrate the complementary and protective role data transparency rights can have, even in those cases where the heightened level of transparency provided by arts 22 and 15(1) h GDPR is not legally mandated. In this regard, see also the discussions under Section 2 and Section 4. Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019 accessed 23 June 2021, paras 4.36, 4.45 and 4.47.

The dimensional analysis should however be understood as dynamic, rather than fixed, exhaustive or definite: we understand that each dimension, and the challenges identified therein, represent but a fraction of elements and that shape the ultimate value and range of data transparency rights. Moreover, any approach towards the enhancement of these rights must allow for a certain level of adaptability in order to account for the fast-changing nature of the digital society.[118] The section will therefore conclude advancing the multidimensional analysis as a modular approach through which data transparency rights can be both critically evaluated and further developed.

4.1 The Data Subject Dimension

The information to be provided in the context of data transparency rights should be evaluated (partially) through the lenses of the data subject's subjective experiences. As mentioned before, the controller must take into account the position and characteristics of the data subject when providing information and explanations. Information should thus be catered to – and evaluated in light of – the wants and needs of the data subject.[119] The subjective experience of the data subject colours the value of data rights in two ways. First, it actively shapes the information they wish to receive. Second, once information is obtained, the effectiveness of data transparency rights will be evaluated in light of how the information received, corresponds to the initial wishes of the data subject, and whether that information helps them in the pursuit of their goals. A data subject might, for instance, be interested to know the categories of personal data collected in the context of a news recommender system without looking for a detailed explanation of the functioning of the underlying ranking system. In that case, the data subject is likely to be satisfied with a clear overview of the categories of personal data processed, together with the purposes and the lawful grounds on which processing is based. This should be made available spontaneously by the controller or obtained through an access request.[120]

The following paragraphs focus on three main (categories of) goals that the data subject might want to pursue. In doing so, we expand upon the goals underlying data protection introduced in Section 2; i.e., transparency, control and power mitigation. These goals can help qualify the specific reasons data subjects may exercise transparency rights for. Unsurprisingly, these goals are also interconnected. Data subject control depends on a minimum level of transparency and both of these are requirements for countering power asymmetries. Information can only be obtained through strong data transparency rights, which requires a robust legal environment.[121] In this regard, the general modalities for the exercise of data rights legally

---

[118] For example, an in-depth exploration of the cultural, political and economic conditions that affect data transparency, including education and digital literacy, could also have been considered. Unfortunately doing so falls outside of the scope of this chapter.

[119] See also: Christopher Kuner and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 7 *International Data Privacy Law* 1, 2.

[120] Of course, other subjective factors, beyond individual goals, can further shape the value of data transparency rights, such as the data subject's educational background, digital literacy or understanding of the law.

[121] See also Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 20–21 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 accessed 26 February 2021.

embed and further solidify the need for data controllers to adequately take into account the data subject's subjective position vis-à-vis information and transparency.[122]

4.1.1 Transparency

As mentioned before, transparency holds both an intrinsic (transparency as an *end*) and an instrumental (transparency as a *means*) value. This has two implications. First, it may inform us how data transparency rights are best evaluated. On the one hand, information can be evaluated in terms of the direct knowledge a data subject is given regarding personal data processing: does the information succeed in making an artificial, and largely invisible process, more observable for the data subject? Here, data transparency rights serve a direct and intrinsic transparency purpose. On the other hand, data transparency rights can be assessed in light of the relevant contribution they make to other goals a data subject might pursue. For instance, having gained insight into the processing of personal data, can the data subject now use that information to exercise their rights and (re)gain control over their data? Put briefly, data transparency rights can be evaluated in function of the support they offer data subjects in light of intrinsic and instrumental transparency goals. This is a functional or goal-oriented evaluation of transparency rights.

Second, as information is meant to inform, protect and empower data subjects, the value information holds is (partially) determined by the perceptions of the individuals on the receiving end. The dual role of transparency may only come to fruition if the data subject is actually capable to both understand and utilise the information provided. Hence, we should ask to what extent transparency requirements should be evaluated through the data subject's (individual) perspective. Where data transparency rights need to enable data subjects to pursue their goals, they might only be effective when the information is sufficiently contextualised to their specific position. In other words, efforts concerning data transparency should not only be functional, but also contextually evaluated. Indeed, to what extent should the controller take into account the specific wants and needs of the data subject when accommodating data rights, and if so, can the controller be held liable or responsible for failing to (sufficiently) do so?[123]

The need to cater information to the specific data subject involved has for example been argued for in the context of ADM, especially where an ex-post explanation is sought.[124] Even

---

[122] GDPR, art 12.

[123] See also section 4.1.4: An Active Role for Data Subjects?

[124] See e.g., Christopher Kuner and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 7 *International Data Privacy Law* 1; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233; Heike Felzmann and others, 'Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns' (2019) 6 *Big Data & Society* 3. Similarly, the need to contextualise information, including explanations, has also been explored in the work of Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2020) *International Data Privacy Law* 125 https://doi.org/10.1093/idpl/ipaa020 accessed 26 February 2021 and Ronan Hamon and others, 'Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 Use Case Scenario', *Proceedings of ACM Facct Conference* (2021 forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3774114 accessed 26 February 2021. For instance, Kaminski and Malgieri propose a multilayered explanation process, which differentiates between a system-level explanation, group-level explanation, and a more granular, individualized explanation. See also literature referenced under (n 97), as well as rulings referenced under (n 2, 87, 93, 111, 117 and 161).

where a decision has not yet been reached, it might be desirable to inform data subjects concerning their specific situation.[125] Should such tailor-made information also be provided for other types of data processing however? Meaningful information, we argue, should not only be provided in cases involving ADM, but should also be extended to any processing activity. With regard to ex-ante transparency requirements, it could be argued that subject-centricity might place a too heavy burden on controllers.[126] Yet, even in those instances, it would be reasonable to expect controllers to adjust the way they comply with transparency requirements according to some tangible metric.

When it comes to ex-post empowerment measures such as the right of access, controllers are in principle able to concretely verify the needs and wants of the data subject and, therefore, can be expected to provide more specific information.[127] One could argue that, as soon as the data have been collected and that the processing has begun, the controller should proactively provide information to the data subject with special attention to their specific situation. For example in the case of profiling, periodic updates could be given regarding inferences made, whereby the necessary information to understand, manage and correct data involved is given to data subjects.[128] The latter example further illustrates the link between transparency and control.

In sum, the efficacy of data transparency rights can be evaluated in terms of their functional and contextual nature. On the one hand, it should be ascertained to what extent information provided contributes to the goals the data subject might pursue. On the other hand, that information should, to the extent possible, be contextualised in relation to the specific position of the data subject and the pursuit of those goals.[129]

---

[125] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233.

[126] Cf. GDPR, arts 24(1), 25(1).

[127] GDPR, Rec 63.

[128] Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 *Law, Innovation and Technology* 266, 282.

[129] There might be limits to contextualisation however. For example, data subjects' 'reasonable expectations' should not be over-relied upon in order to interpret or accommodate data transparency rights as these expectations might be subject to external manipulation. Van Ooijen and Vrabec, in reference to Chartrand, note that the attitudes and preferences of data subjects may be 'the result of cognitive processes, wherein an individual was not "in control" of information'. I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, at footnote 4. T L Chartrand, 'The Role of Conscious Awareness in Consumer Behaviour' (2005) 15(3) *Journal of Consumer Psychology* 203–210. Likewise, one could consider the problem of adaptive preferences as described by Jon Elster. The latter refers to the idea that people might alter their preferences on the basis of the alternatives they have available, or the lack thereof. People might also adapt their preferences in response to a generally unfavourable environment, accepting, rather than fighting against the negative consequences this environment bears for them. Applied to this particular case, data subjects might have reduced expectations vis-à-vis transparency because they were never given proper information or transparency to begin with. If people do adapt their preferences to what is possible for them, perhaps then, one can question the general reliability of people's wants and preferences as a (sole) metric for evaluation. See *among others* Jon Elster, *Sour Grapes: Studies in the Subversion of Rationality* (Cambridge University Press 2016), *among others* at 22 and 109, https://www.cambridge.org/core/books/sour-grapes/F2076EE5F87E99C6A47C708D7D99509A accessed 21 February 2021; Ben Colburn, 'Autonomy and Adaptive Preferences' (2011) 23 *Utilitas* 52. Miriam Teschl and Flavio Comim, 'Adaptive Preferences and Capabilities: Some Preliminary Conceptual Explorations' (2005) 63 *Review of Social Economy* 229. Of

4.1.2 Control

The ability to exercise control over the use of data is one goal for which access to information is a necessary precondition.[130] Van Ooijen and Vrabec for example note that data subjects maintain control over their data if they can make decisions regarding data processing activities that reflect their existing attitudes and preferences.[131] As a minimum, they observe, data subjects should be sufficiently aware of what the processing of their data entails.[132] As the conduit to such information, data transparency rights are indispensable tools towards data subject empowerment. In order to establish control, however, they should not only render data processes intelligible in terms of their functioning, but also in terms of their concrete impact. Only then can data subjects concretely assess what is at stake, and why control might be needed. Furthermore, practical insight should be given regarding the tools through which the data subject can exercise control, such as through data rights. Indeed, control may manifest itself in many ways, and data subjects might want to exercise control in many different ways. Data subjects might want to erase, correct or transfer certain data, and/or restrict or object to specific processing operations. Data transparency rights again appear in need of a functional and contextual interpretation.

Common transparency obstacles, such as information complexity and/or overload,[133] might appear to severely thwart data transparency rights' instrumental function of enabling control. Yet, we argue that such obstacles do not render the contribution of data transparency rights obsolete. Indeed, in many situations they either do not fully apply, or can be easily overcome. *First*, there are concrete instances imaginable where control is sought and where the data processes involved are not overly complex and easily manageable via transparency rights. For example, a data subject might issue an access request with a local bakery or insurer out of fear that these local entities have sensitive information that could cause reputational damage on a local level. In this particular case, the data subject acts upon intuition. The access request is likely not motivated by an extensive investigation into a set of dense and complex data policies. Indeed, data subjects may not actively look for comprehensive control, but may simply be confronted with specific instances where they desire control. It is at this point in time, that data subjects value the presence and their ability to rely upon strong data transparency rights. When they are called upon – which might not necessarily be in relation to an overly complex processing operation – data transparency rights should be able to perform their function.

---

course, the aforementioned can be seen as an additional challenge that must be overcome: to place data subjects in a position where they know and understand the importance of their rights.

[130] See also: Section 2.2 Control and I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91.

[131] Albeit again that data subjects may not always be in full control of these preferences, see I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, 94; and observations made at (n 129).

[132] I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, 94. In their article, van Ooijen and Vrabec investigate whether the GDPR can effectuate individual control (over consent-based processing) from a behavioural perspective.

[133] See also I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, 94–96, who discuss how information complexity and overload can threaten data subject control (n 129).

Second, having identified obstacles towards control, it should be investigated how data transparency rights can best help to overcome these challenges and, more specifically, 1) which tools available to the data subject are the most appropriate to realise control, 2) what are the most efficient means to raise awareness amongst data subjects regarding the existence of these tools and 3) at what point in time throughout the course of the personal data processing life cycle are data subjects most receptive to this type of information. The answers to the above-mentioned questions might differ depending on the stage of the data process under investigation.[134] This functional and contextual approach allows to focus on the further development of data transparency rights in a goal-oriented manner. Data transparency rights can thus become more effective either because the information they convey directly contributes to the exercise of control, or because the information directs data subjects towards the tools through which they can further exercise control.

4.1.3 Power imbalances

Whereas a data subject might regain control over their data, this control takes place on an individual level and does not yet restore the power imbalances present in the digital environment. Informational power asymmetries can only be countered via strong transparency measures. The importance of data transparency rights, and the right of access in particular, should not be underestimated. Indeed, a growing range of initiatives (led by a variety of actors, from individuals, to NGOs, journalists and academics) make creative use of data transparency rights in order to tackle negative externalities stemming from power asymmetries.[135]

While the data subject is traditionally perceived as a singular entity, the GDPR nonetheless provides the tools for data subjects to gain strength in numbers through concerted efforts. The GDPR explicitly recognises the value of collective action in Article 80, which allows data subjects to mandate a non-profit in the exercise of certain rights.[136] Group representation is but

---

[134] For example, van Ooijen and Vrabec have mapped threats to individual control in relation to different stages of data processing (the information receiving stage, the approval and primary use stage and the secondary use of data stage). Having investigated these three different stages, they found that depending upon the stage under scrutiny, certain tools within the GDPR might offer better (individual) control than others. They found for instance that both the right to an explanation and data protection by default could have the potential to effectuate individual control, but at different points in time; also I van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, 103–105.

[135] See for an overview: René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020). See also the Amsterdam's District Court's rulings under (n 2, 87, 93, 111, 117 and 161). The Worker Info Exchange, for example, collects and pools data from gig economy workers in order to improve their working conditions vis-à-vis the platforms and entities that control and manage their activities. In this regard, (group) access requests are one tool through which more transparency over working conditions can be obtained; https://www.workerinfoexchange.org/ accessed 5 July 2021.

[136] GDPR, art 80. As an example of collective action, reference can be made to the fine imposed by French national supervisory authority CNIL on Google LLC. This fine was, *amongst others*, kickstarted by group complaints from associations None of Your Business and La Quadrature du Net. The latter was mandated by 10 000 people; CNIL, 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC' (21 January 2019) https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc accessed 26 February 2021; A 'GDPR class action' has also been filed against Oracle and Salesforce: Natasha Lomas, 'Oracle and Salesforce hit with GDPR class action lawsuits over cookie tracking consent.' (14 August 2020,

one way through which data subjects can be empowered. As noted by Mahieu and Ausloos, the GDPR provides an 'architecture of empowerment' with a strong collective dimension that has, up until this point, remained understated.[137] They argue that the right of access is pivotal in democratising control over data processing in a digital society.

In related empirical research concerning the collective exercise of the right of access, Mahieu and others also found that access rights should not be devalued, even though they are seldom complied with in practice:

> When the right is used in a collective manner, it creates a context to judge the quality of replies and the lawfulness of the data practices by comparing replies to similar access requests. Participants also perceived a societal much more than an individual value in exercising this right, not [in] the least because through collective use, the power imbalance between individual citizens and organisations shifts in favour of the citizen.[138]

Even in case of non-compliance, they can bring to light valuable information regarding the (the lack of) organisational and technical measures in order to ensure data protection compliance. Collective approaches acknowledge the difficulty that access rights might face on the individual level, but they are able to turn those into informational power. Indeed, claims for non-compliance will be even stronger when substantiated by numerous different (failed) attempts at exercising data transparency rights.[139]

4.1.4 An active role for data subjects?

The goals data subjects may pursue with their data transparency rights can be roughly categorised along the three aforementioned overarching data protection goals: transparency, control and power mitigation. As indicated above, there have been discussions as to whether information should be contextualised to the data subject, and if so, to what extent, and by what means. To focus on the aforementioned goals then offers the practical advantage that it (partially) offsets the main difficulty of measuring, and subsequently accommodating, the

---

TechCrunch); https://techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/?guccounter=1 accessed 28 November 2020.

[137] René Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020).

[138] René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 *Internet Policy Review* 17 https://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect accessed 26 February 2021.

[139] At the same time, the GDPR has also been criticised for lacking an explicit collective dimension, especially in relation to Big Data analytics. In this context, discussions have been held regarding the potential value of group-related (and the deficits of individual) notions of privacy and data protection. See for example the following literature: Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer International Publishing 2017) http://link.springer.com/10.1007/978-3-319-46608-8 accessed 21 February 2021; Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 *Ethics and Information Technology* 275; Laurens Naudts, 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them' in Ronald Leenes and others (eds), *Data Protection and Privacy : The Internet of Bodies* (1st edn, Hart Publishing 2019) http://www.bloomsburycollections.com/book/data-protection-and-privacy-the-internet-of-bodies/ch3-how-machine-learning-generates-unfair-inequalities-and-how-data-protection-instruments-may-help-in-mitigating-them/ accessed 21 February 2019.

subjective expectations of data subjects.[140] Instead, the goals represent a tangible proxy for the expectations of data subjects and can be anticipated.[141] In the meantime however, it remains valuable to look for new ways to meaningfully involve data subjects in shaping the ways information is provided.[142]

The challenge of how, and through which means, data subject preferences can be assessed and accommodated is not necessarily a legal one, and is likely to require significant inter-disciplinary research.[143] A heightened focus on user-experience can be found in the field of human-computer interaction, where use is made of, *inter alia*, co-design strategies in an effort to actively seek end-user engagement and participation throughout the design process.[144] In such a co-design approach, users are seen as partners and actively involved in the design process as 'experts of their experience'.[145] Co-design workshops for instance invite end-users to participate as co-creators in the design process through a series of reflective exercises, ideating applications and design features among others.[146] Through these activities, end-users are

[140] Where the ex-post right to access is concerned, expectations can be more explicitly communicated by the data subject to, or measured by, the controller. In the latter instances, it could be argued that the expectations of data subjects should be actively ascertained by the controller.

[141] Of course, these expectations might already be shaped by the nature of the rights in question. It seems reasonable to assume that transparency rights will be exercised by data subjects for transparency and for transparency-related purposes, or purposes for which information is needed.

[142] At the same time, and as aforementioned, research might equally identify those areas where data subject expectations are better not to be taken into account.

[143] Measuring such expectations might also introduce legal challenges, including data protection related ones; e.g.: measuring expectations ex-ante might require additional personal data to be collected.

[144] See e.g.: Clay Spinuzzi, 'The Methodology of Participatory Design' (2005) 52 *Technical Communication* 163; Maarten Van Mechelen and others, 'The GLID Method: Moving from Design Features to Underlying Values in Co-Design' (2017) 97 *International Journal of Human Computer Studies* 116; Q Vera Liao and Michael Muller, 'Enabling Value Sensitive AI Systems through Participatory Design Fictions' 7. Andrés Lucero and Tuuli Mattelmäki, 'Good to See You Again: Engaging Users in Design', *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces - DPPI '11* (ACM Press 2011) https://dl.acm.org/citation.cfm?doid=2347504.2347517 accessed 26 February 2021; Oscar Alvarado and others, 'Foregrounding Algorithms: Preparing Users for Co-Design with Sensitizing Activities', Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (Association for Computing Machinery 2020) https://doi.org/10.1145/3419249.3421237 accessed 29 June 2021.

[145] Froukje Sleeswijk Visser and others, 'Contextmapping: Experiences from Practice' (2005) 1 *CoDesign* 119; Elizabeth B N Sanders and Pieter Jan Stappers, 'Co-Creation and the New Landscapes of Design' (2008) 4 *CoDesign* 5, at 8 and 12.

[146] See *among others:* Maarten Van Mechelen and others, 'Collaborative Design Thinking (CoDeT): A Co-Design Approach for High Child-to-Adult Ratios' (2019) 130 *International Journal of Human-Computer Studies* 179, 181. Andrés Lucero and Tuuli Mattelmäki, 'Good to See You Again: Engaging Users in Design', *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces - DPPI '11* (ACM Press 2011) https://dl.acm.org/citation.cfm?doid=2347504.2347517 accessed 26 February 2021; Oscar Alvarado and others, 'Foregrounding Algorithms: Preparing Users for Co-Design with Sensitizing Activities', Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (Association for Computing Machinery 2020) https://doi.org/10.1145/3419249.3421237 accessed 29 June 2021. Other co-design approaches exist as well, such as probes and toolkits. See e.g.: Elizabeth B N Sanders and Pieter Jan Stappers, 'Probes, Toolkits and Prototypes: Three Approaches to Making in Codesigning' (2014) 10 *CoDesign* 5.

given the opportunity to collaborate in, and give shape to, the design of a particular process.[147] Such participatory methods could also be explored as a means to actively engage data subjects and draw from their experiences to further inform the ways information can be communicated as part of data transparency rights. A three-tiered process of participation, iteration and validation could further help to ensure that throughout the design process the data subject's position is not only taken into account, but also verified and validated. These methods are but one potential direction forward and they could co-exist or be combined with other interdisciplinary initiatives towards enhanced and automated transparency.[148]

Participatory strategies could also be tested in those areas where the GDPR encourages active data subject involvement. Recital 99 GDPR for instance notes that, when efforts are made to formulate a code of conduct, relevant stakeholders, including if feasible data subjects, should be consulted.[149] Similarly, in cases of high-risk data processing, the controller should seek the views of data subjects where appropriate as part of a data protection impact assessment.[150] Likewise, participatory design could inform data protection by design.[151] Data subject involvement could thus become a meaningful form of engagement that allows controllers to better assess and respond to the wants and needs of data subjects.[152]

4.2 The Legal Dimension

The GDPR – let alone the individual data transparency rights within it – does not operate in a vacuum. Instead, the efficacy of the GDPR' transparency toolset is shaped by the environment in which data subjects and the law operate. Still, in this section, we present how, as part of the multidimensional approach, the legal dimension too can be used as a means to critically reflect upon data transparency rights. Rather than critically investigate data transparency rights in isolation, we discuss two challenge areas related to the application of the law as a discipline. Research within these areas could further improve the value and function of these rights: the conceptual interpretation of data transparency rights and the temporal dynamics of the rights in question.

---

[147] For an example of other processes that could be involved in participatory design strategies, reference can be made to the work of Alvarado and others. They stress the importance of sensitising activities, which serve to raise awareness and knowledge among research participants in areas they might be unfamiliar with, such as the functioning of algorithms. Such sensitising activities can be seen as a first step to facilitate co-design. Oscar Alvarado and others, 'Foregrounding Algorithms: Preparing Users for Co-Design with Sensitizing Activities', Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (Association for Computing Machinery 2020) https://doi.org/10.1145/3419249.3421237 accessed 29 June 2021.

[148] See e.g., P Murmann and S Fischer-Hübner, 'Tools for Achieving Usable Ex Post Transparency: A Survey' (2017) 5 *IEEE Access* 22965. See also Section 4.3 'The Socio-Technical Dimension'.

[149] GDPR, Rec 99 and art 40(2)(a). A code of conduct may specify what should be understood as fair and transparent data processing.

[150] GDPR, art 35(9).

[151] GDPR, art 25.

[152] At the same time, one should keep into account the aforementioned pitfalls concerning the rationality of data subjects mentioned at (n 129).

4.2.1 Interpretation of the law

The GDPR's transparency requirements contain many concepts that are subject to interpretation and have not yet been fully clarified. While the CJEU has already provided some clarification on the meaning of transparency and the right of access, conceptual confusion still subsists with regard to other concepts.[153] No clear consensus exists on the exact scope or meaning of notions like 'categories of data', 'meaningful information', 'logic involved' or 'envisaged consequences'.[154] Future case-law will have an important interpretative function in this regard. Similarly, guidance provided by the European Data Protection Board, albeit non-binding, does hold considerable level of authority. As the law continues to evolve, two additional observations can be made: one relates to the role of other disciplines, and the other to the nature of the legal concepts at stake.

Controversies on the interpretation of legal notions differ from parallel discussions held in other disciplines regarding identical – or at least comparable – concepts. The 'meaningfulness' of explanations, for instance, has been subject to debate in philosophy, social, cognitive and computer sciences – disciplines far more apt than the law to provide concrete building blocks towards achieving transparency on a cognitive level.[155] On a technical level, interdisciplinary efforts towards explainable artificial intelligence (XAI) are particularly interesting to follow.[156] Research should not only seek ways to accommodate data subjects' expectations, however.[157] As hinted above, critical questions could be raised as to whether the subjective experiences of the data subject should be given priority. Similarly, it could be investigated to what extent these expectations can be manipulated by controllers. Still, other disciplines should certainly play a role in informing the further development and understanding of the law and the obligations contained therein. Whereas the law can provide a framework to help operationalise scientific knowledge from other disciplines concerning the provision of meaningful information, this knowledge could also be harnessed to further strengthen the protection the law seeks to afford. For example, if a study was to uncover that data subjects are best informed concerning the envisaged consequences of ADM through visual icons, the legal notion of

---

[153] See e.g., the following cases from the Court of Justice: Case C-553/07 *College van burgemeester en wethouders v M.E.E. Rijkeboer* [2009]ECLI:EU:C:2009:293 (Rijkeboer); Joined Cases C-141/12 and C-372/12 *YS and Others v Minister voor Immigratie, Integratie en Asiel* [2014] EU:C:2017:994 and Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994 (Nowak).

[154] For an exploration of the relationship between categorising data, transparency and the obligation to inform, see also: Emma Cradock, Sophie Stalla-Bourdillon and David Millard, 'Nobody Puts Data in a Corner? Why a New Approach to Categorising Personal Data Is Required for the Obligation to Inform' (2017) 33 *Computer Law & Security Review* 142.

[155] James Woodward, 'Scientific Explanation' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Winter 2019, Metaphysics Research Lab, Stanford University 2019) https://plato.stanford.edu/archives/win2019/entries/scientific-explanation/ accessed 1 September 2020; Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences' [2017] arXiv:1706.07269 [cs] http://arxiv.org/abs/1706.07269 accessed 26 February 2021; Tania Lombrozo, 'The Instrumental Value of Explanations' (2011) 6 *Philosophy Compass* 539.

[156] Motahhare Eslami and others, 'Communicating Algorithmic Process in Online Behavioral Advertising', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018) http://doi.acm.org/10.1145/3173574.3174006 accessed 17 May 2018; Oscar Alvarado and Annika Waern, 'Towards Algorithmic Experience: Initial Efforts for Social Media Contexts', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018) http://doi.acm.org/10.1145/3173574.3173860 accessed 17 May 2018.

[157] See also *supra* Section 4.1.4. 'An Active Role for Data Subjects?' and observations under (n 129).

'meaningful information concerning the envisaged consequences' could be interpreted as an obligation to operationalise transparency through icons.

At the same time, the law itself puts forward its own goals and purposes. These particular goals may equally inform the interpretation of the notions that the law has introduced. For example, whether information is meaningful within the sense of the GDPR should not only be understood in relation to the data subjects' cognitive abilities to capture the envisaged consequences on a technical (what is the logic involved?) or outcome-based (will a loan be granted or not?) level. Information can and should be understood functionally, in relation to the goals of the data subject, but also in relation to the goals pursued by the law (in casu, the GDPR). Another example concerning the provision of plain and intelligible information can be found in consumer protection law. In the *Kásler* case, the CJEU had to interpret the conditions under which contractual terms are clear and intelligible.[158] The Court noted that the requirement for a contractual term to be drafted in plain, intelligible language does not only require that the relevant terms are intelligible for the consumer in a grammatical sense. Rather, contractual terms should set out in transparent manner the specific functioning of the contractual mechanisms at play, as well as the relationship between those mechanisms and those provided for by other contractual terms in order to allow the consumer to evaluate, on the basis of clear and intelligible criteria, the actual economic consequences that follow from the contract.[159] In other words, intelligibility seems to require not only the implementation of mechanisms that allow cognitive understanding, but also a functional understanding; an understanding in function of the goals and values a particular law seeks to protect.[160] An equivalent argument can now be drawn with regard to the GDPR's transparency rights: transparency requirements should be interpreted so that they enable the manifestation of the values and objectives underlying the GDPR. Similarly then, data transparency rights should be interpreted in such a way that they can effectively be used by the data subject in order to pursue the goals and interests envisaged by these rights. All things considered, data transparency rights should at least 1) offer data subjects a concrete means to make the processing operations they are subject to more tangible; 2) empower data subjects in terms of the control they have over their data; and 3) contribute to breaking down data-driven power asymmetries.[161] Similarly, the information conveyed

---

[158] Case C-26/13 *Árpád Kásler and Hajnalka Káslerné Rábai* [2014] EU:C:2014:282 [2014] (Kásler), para 75. For a more in-depth investigation of citizen empowerment in relation to consumer and data protection law, including the aforementioned Kásler case, see also: Clifford, Damian, Data Protection and Consumer Protection: The Empowerment of the Citizen Consumer (May 27, 2020), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds), Edward Elgar Publishing (Forthcoming), ANU College of Law Research Paper No. 20.11, Available at SSRN: https://ssrn.com/abstract=3611436 accessed 26 February 2021.

[159] Kásler, para 75.

[160] See also Damian Clifford, Data Protection and Consumer Protection: The Empowerment of the Citizen Consumer (May 27, 2020).

[161] Such information could already be given as part of the ex-ante transparency requirements, where data subjects must be informed on the existence of their data rights (GDPR, arts 13(2)(b) and 14(2)(c)). Similarly, with regard to the rights of the data subject, one could argue that the provision of such goal-oriented information can be seen as a further clarification of the requirement that any communication under arts 15–22 need to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. See GDPR, art 12(1). As aforementioned, the Uber and Ola rulings of Amsterdam's District Court too can be seen as illustrating the importance transparency holds

through data transparency rights should allow data subjects to understand the conditions under which they can further bolster their protection.[162]

Further interpretative guidance may also be developed through self- and co-regulatory initiatives. For example, the GDPR encourages associations and other bodies representing categories of data controllers or processors to develop codes of conducts, which could specify *among others* the meaning of fair and transparent processing, and the information that ought to be provided to the public and data subjects.[163] Developments in XAI, and their uptake by controllers, could also affect the ways in which data subject receive, perceive and process information, and as such, introduce new transparency benchmarks.[164]

4.2.2 Time of exercise

Data transparency rights can be triggered at different points in time.[165] As data processing activities evolve over time, so do the associated personal data and the constellations of actors involved.[166] In order to preserve the contextual and functional nature of information, changes that take place over time should also be reflected through the various transparency mechanisms. Unfortunately, the shifting dimensions of personal data (processing) over time are not always sufficiently acknowledged, despite the advantages this would grant in relation to the

---

for digital rights (n 2, 87, 93, 111 and 117). For example, transparency's protective and empowering function seemed to be recognised where the Court concluded that Ola had to provide drivers access to data used for their system's fraud probability score and earning profile on the basis of art 15 GDPR's general transparency requirements. Said information was deemed necessary for drivers to verify the correct nature of the data used by the profiling processes, and the segments into which they were classified. Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1019,https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019 accessed 23 June 2021, paras 4.36, 4.45 and 4.47. Similarly, in one of the rulings against Uber, the Court concluded that certain drivers were given insufficient information regarding the fraudulent behaviour that was at the basis of their account's deactivation. Uber was ordered to provide access to the personal data upon which the deactivation was based so that the drivers could verify whether the processing of their data was correct and lawful. Rb. Amsterdam 11 March 2021, ECLI:NL:RBAMS:2021:1018 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1018 accessed 23 June 2021, paras 4.29 and 4.32.

[162] Discussions regarding the right to access may also be used to argue in favour of the fact that information should support the objectives of the law. The right to access has, next to granting access to information, a secondary, enabling function: to facilitate the exercise of the other data subject rights, such as the right to object. This 'enabling role' was also recognised by the CJEU in the *Rijkeboer* ruling. Case C-553/07 *College van burgemeester en wethouders v. M.E.E. Rijkeboer* [2009]ECLI:EU:C:2009:293, paras 51–52.

[163] GDPR, art 40.

[164] Wachter and Mittelstadt e.g., have proposed a right to reasonable inferences, which would include a right to know about inferences as a means to cover some of the GDPR's transparency loopholes where inferential analytics and profiling are concerned. Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) *Columbia Business Law Review* 494, 545–548.

[165] See *supra* Section 3 'Data Transparency Rights: The Legal Framework', and more specifically, the distinction between ex-ante and ex-post provisions.

[166] Inferential analytics for instance, give controllers the opportunity to better understand data subjects, their goals and motives, which might differ from the moment their personal data were initially collected.

aforementioned goals of the data subject, and the need for functional and contextual information therein.[167]

The need to provide time-specific information should therefore be further encouraged.[168] Such temporal dynamism should become an essential component of data transparency rights, especially when it comes to ex-post mechanisms. The right of access, for instance, can capture *at least* every processing instance that takes place after data collection. Moreover, the right can be exercised periodically, which could grant data subjects the opportunity to obtain different, contextualised information every time the right is exercised. At the same time, the amount of information that can be provided ex-ante should not be underestimated, even where complex systems are involved. Powles and Selbst, for example, note that many complex applications remain deterministic and therefore predictable. As a result, a complete system-level explanation should tell a data subject everything they need to know about the specific operations that follow from such deterministic systems.[169] Still, only ex-post information can truly complement contextualised transparency by introducing temporal dynamism.

In this regard, transparency should not be seen as an obligation that prescribes the provision of a fixed set of information to be given at specific points in time only. Instead, and alongside the aforementioned phases of ex-ante and ex-post transparency, it is important to recognise transparency as a dynamic and continuous process. Such dynamism may reinforce data subjects' control. In principle, it should allow the data subject to more easily assess when it might be beneficial to withdraw from a given processing activity. For example, as soon as it appears from the information provided that the controller's operations no longer correspond to the data subject's initial wants, needs or expectations. As a consequence, the value of ex-ante information might also increase. Indeed, ex-ante information could then serve as the baseline against which data subjects can map and evaluate all subsequent actions of the controller.[170]

4.3 The Socio-technical Dimension

Data transparency rights are not just affected by data subjects' expectations (Section 4.1) or the wider legal environment (Section 4.2), but they also face a number of obstacles, arising from the interaction between data subjects and controllers (relational obstacles) and/or the technologies they use (infrastructural obstacles). The sum of these interactions constitutes

---

[167] For example, in the authors' (empirical research) experience with access requests, data controllers often argue that the information provided under art 15 should not be considered different from the information that needs to be provided under arts 13(2)f and 14(2)g. For an illustration of the empirical research activities of the authors, reference can be made to: Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4.

[168] See also Section 4.1.4 'An Active Role for Data Subjects?'. For example, if the data subject exercises their transparency rights with a particular goal in mind, the ex-post nature of the right to access allows the data controller to take into account the data subject's specific needs when granting the request.

[169] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 239, in reference to E Horvitz, 'On the Meaningful Understanding of the Logic of Automated Decision Making' BCLT Privacy Law Forum, 24 March 2017 https://www.law.berkeley.edu/wp-content/uploads/2017/03/BCLT_Eric_Horvitz_March_2017.pdf accessed 23 February 2020.

[170] Of course, the mode or format through which information is given would need to follow and account for this dynamism. In an ever-changing environment, visual cues might be more easily provided and understood than textual ones.

a socio-technical dimension that further affects the exercise and operationalisation of data transparency rights.

The socio-technical dimension captures a highly intertwined technologically co-shaped environment through which data subjects must navigate. As such, this dimension illustrates quite well how data transparency rights do not operate within a vacuum: data subjects navigate within an environment co-shaped by a variety of (f)actors beyond their control. The data subject's socio-technological interactions can furthermore be embedded into a wider, socio-economic and even political context, which would bring even more challenges to the forefront. Such a large-scale endeavour, which does indicate the fluidity of the dimensions involved, unfortunately falls outside the scope of the current contribution.[171] Nevertheless, it is worth considering the aforementioned relational and infrastructural obstacles – both in isolation and in their interaction – as they directly oppose the data subject in the exercise of their data transparency rights. By way of example, two oft-heard criticisms regarding the efficacy of transparency rights can be highlighted here: a lack of compliance among controllers on the one hand (relational), and the complexity of processing systems on the other hand (infrastructural). Related to the socio-technical environment, they could be seen as arguments against the value of data transparency rights.

First, a controller's compliance with and interpretation of the GDPR greatly affect the information a data subject can effectively obtain. More often than not, controllers' systematic failure to appropriately accommodate access requests[172] is symptomatic of inadequate enforcement rather than alleged ambiguities in the text of the GDPR. While controllers have been fined for their lack of transparency, further measures to ensure respect for data transparency rights could be taken.[173] As enforcement takes place on a national level, a harmonised approach would further reduce disparity in data subject transparency. In cross-border data protection cases, the national supervisory authorities, should moreover cooperate in order to

---

[171] For example, we could highlight the importance of education and digital literacy. Data subjects might have a strong set of data transparency rights, but if they are unaware these rights exist, they will never be exercised. Likewise, data subjects might know and understand their individual rights under the law, but the current political regime might not prioritise their enforcement, making them de facto obsolete. See also Joanna Strycharz, Jef Ausloos and Natali Helberger, 'Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR' (2020) 6 *European Data Protection Law Review* 407. The aforementioned observations clearly illustrate why we opted for the notion multi-, rather than three-dimensional. As aforementioned, the three dimensions presented here are neither exhaustive, nor definite, and one could think of numerous other 'dimensions' to add to the approach, or to expand the dimensions presented with additional observations. For an alternative exploration of transparency as a relational concept that can be placed within a multi-stakeholder environment, see also: Heike Felzmann and others, 'Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns' (2019) 6 *Big Data & Society* 1.

[172] See e.g.: René L P Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 *Internet Policy Review* 3; Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8(1) *International Data Privacy Law*.

[173] Alex Hern, 'Google Fined Record £44m by French Data Protection Watchdog' *The Guardian* (21 January 2019) https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog accessed 12 October 2020.

ensure the consistent application of the GDPR.[174] Discrepancies could furthermore be resolved through the consistency mechanism, which grants the European Data Protection Board the possibility to issue opinions, or in case of disputes between national DPAs, binding decisions as an arbitration measure.[175] Up until the moment binding guidance is issued, controllers of course have room for manoeuvrability regarding the information they wish to provide. In addition, the Court has acknowledged that data protection laws have to be interpreted also in relation to the responsibilities, powers and capabilities of the data controller.[176] Still, the freedom of the controller should not unduly reduce the value of data transparency rights: as aforementioned, even the bare minimum information provided should result in a sufficient level of understanding among and serve to empower data subjects.[177]

Second, it might be argued that the complexity of technologies does not allow proper information to be provided. While the use of complex technologies should not limit the rights of the data subject,[178] the capacity to provide information in an intelligible manner might become more difficult.[179] A precondition for the use of a technology might therefore be to have transparent information concerning a technology's functioning and impact in the first place. We would argue that, at the very least, controllers need to communicate to data subjects, ex ante, the exact scope of their data transparency rights, and the potential limitations thereof in light of technological complexity.[180] Adequate safeguards must also be maintained in those cases where the actual appeal of the technologies involved partially stems from their invisibility, and associated lack transparency, such as ambient intelligence or IoT devices.[181] Even if the controller takes sufficient measures, the data subject might not properly understand the processes

---

[174] GDPR, Chapter VII.

[175] GDPR, art 64. See also, for an overview of the decisions adopted under the consistency mechanisms: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en accessed 26 February 2021.

[176] Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014]; ECLI:EU:C:2014:317, para 83; and r136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] EU:C:2019:773, paras 47–48.

[177] The CNIL fined Google *amongst others* for exactly this omission. The CNIL observed that Google had violated transparency and information obligations because 'the purposes of processing [were] described in a too generic and vague manner, and so [were] the categories of data processed for these various purposes'. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc accessed 26 February 2021. See also section 4.2.1: 'The Interpretation of the Law.'

[178] Jef Ausloos, 'Paul-Olivier Dehaye and the Raiders of the Lost Data' (*CITIP blog*, 10 April 2018) https://www.law.kuleuven.be/citip/blog/paul-olivier-dehaye-and-the-raiders-of-the-lost-data/ accessed 21 February 2021.

[179] See e.g.: Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012* (First, IOS Press 2012); Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 *Law, Innovation and Technology* 266.

[180] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International Data Privacy Law* 4, 14 et seq; Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2020) 10 JIPITEC 307.

[181] See: Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 *Law, Innovation and Technology* 266, 267. As observed by Wachter, a 'fundamental tension exists between the seamless and non-transparent nature of the IoT, and the need to keep users informed and in control'.

involved. Hence, developments in XAI, or other relevant scientific domains, could ensure that where new technologies are rolled out, they can be implemented with sufficient guarantees for the involved data transparency rights.[182] Where transparency enhancing design solutions are sought, an appropriate level of subject-centricity should be maintained.[183]

The aforementioned examples concerned challenges related to social actors and technological artefacts in isolation. In reality, controllers, and the technological artefacts they employ, take an active part in, and help co-shape, the wider socio-technical, and also economic environment, in which data subjects find themselves. Data processes, including actors and technologies involved, have become increasingly interconnected. The resulting network is not constituted by single, isolated actors, but rather forms a highly intertwined and dynamic digital eco-system. These complex interrelations might equally encumber the provision of meaningful information. For example, where interconnected ADM systems have been deployed by a constantly changing constellation of separate actors, does an access request only relate to the specific ADM process deployed by the controller that is targeted by the request, or should that controller also aim to provide insight into all other related data processes too?[184] And if so, how can such a level of transparency be achieved in practice? In addition, given the interconnected nature of the digital environment, the wider societal implications of certain data processes should not be underestimated. These implications might not always come to the forefront through individual data transparency rights, even when they are exercised collectively. For example, the impact of a given data process on vulnerable groups of individuals might be of general interest to data subjects, but will often be left unstated. Indeed, such information would typically not be considered as the type of information that is captured under, and should be given via, data transparency rights. The latter two points moreover illustrate that data transparency rights alone might not always be proficient in rendering visible the invisible.

4.4 Data Transparency Rights as Versatile Tools in a Multidimensional Environment

The three dimensions highlighted above – data subject, legal and socio-technical – provide a conceptual lens through which data transparency rights can be assessed, evaluated and improved upon.

Depending on the type of information data subjects seek to receive, and the goals they want to pursue, data transparency rights can be leveraged in different ways and with varying degrees of success. Transparency is a multi-tiered process that holds both intrinsic and instrumental value. In this context, data transparency rights in particular, can generate a wide awareness of data infrastructures, while at the same time offering the ability to scrutinise these data infrastructures for those who want to dig deeper. The knowledge gained through data transparency rights can, in turn, empower data subjects and serve to constrain data-driven power asymmetries. Put differently, data transparency rights operationalise transparency, and in doing so,

---

[182] See also GDPR, art 25(1)); and Sections 4.1.4. 'An Active Role for Data Subjects' and 4.2.1 'The Interpretation of the Law'.

[183] For example, the danger exists that attempts to 'automate' the provision of information result in a loss of contextualisation in favour of efficiency.

[184] Likewise, where data have not been obtained from the data subject, what is the level of provenance or information a controller should provide regarding preceding processing activities under art 14 GDPR?

they can unlock different layers of the transparency process. In this sense, transparency rights could be seen as gradational: starting from insight, they enable data subjects to dig deeper, to facilitate and enable control, and to equalise power asymmetries. Still, while access to adequate information is often seen as a necessary condition towards achieving the latter two goals, data transparency rights do not need to be accommodated in a specific or sequential order in order to contribute to them. In fact, these goals could also be pursued in parallel or in isolation. The aforementioned research into the collective exercise of access rights serves as a prime example. The collective exercise of access rights can lay bare the deficiencies of the digital environment and in doing so help to equalise power asymmetries. Here, data transparency rights transcend their individual nature as an informational tool, gaining a societal function, even if on the individual level information remains lacking.

The multidimensional prism offers a more nuanced perspective of data transparency rights, through which their versatility can be critically reflected upon, evaluated and further developed in a contextual, goal-oriented and functional manner. The dimensions reveal an interconnected and interdependent playground wherein a variety of factors can affect the efficacy of data transparency rights in the pursuit of transparency and transparency-related goals. For example, the highly-intertwined dynamic nature of the digital environment (the socio-technical dimension) is likely to obstruct data subject control (the data subject dimension) if the information controllers need to provide following a data transparency request does not need to take into account how the processing of personal data has evolved over time (the legal dimension). The multidimensional approach could be seen both as a challenge and an opportunity. While it presents a complex research setting, advancements made in one dimension might spill over into the others. In this regard, the dimensions constitute interpretational lenses giving shape and meaning to the rights in question, and the limitations they currently may face. For instance, data subjects may only consider data transparency rights to empower them in a limited set of circumstances, where actual processing operations are not overly complex. Or, where these rights are exercised to mitigate power asymmetries, this function might only come to fruition through a concerted, rather than a singular, exercise of rights, targeting multiple interconnected actors. Because these dimensions can be used to critically reflect upon data transparency rights, the approach may also guide future research by providing a theoretical and practical framework through which data transparency rights can be further developed. Beyond scholarship and research, other stakeholders can utilise a dimensional outlook to their advantage. Data subjects might better understand where transparency rights are most efficient and focus their attention accordingly. National supervisory authorities can enforce data transparency rights in a more targeted fashion, focusing on those barriers that impede transparency rights. Controllers can then adjust their compliance strategies in order for transparency rights to gain actual meaning.

As aforementioned, we do not present these dimensions as exhaustive or definite, and we invite future research to expand or even add new dimensions (e.g., educational, political). While, we argue, the dimensions identified in this contribution are the most apparent ones, we also recognise that they can be 'fluid' in their actual content, and subject to change. For example, the ways in which data processing technologies are employed, and the ways in which these technologies interact with their environment, continuously evolve. In light of such developments, the perception of transparency as a societal value is likely to change as well. In this regard, the multidimensional framework, while modular, offers a nuanced, contextual and

goal-oriented approach through which both the importance of data transparency rights, and the conditions under which they can flourish, take centre stage.

Finally, in light of subsequent research, we want to emphasise the benefits of approaching data transparency rights as versatile and goal-oriented. First, we believe such an approach represents a positive ideal, whereby rights are seen primarily as multi-functional tools that can help inform and empower data subjects. While they may vary in efficiency depending on the context in which they are exercised, their value remains undebated. Second, by focusing on their versatility, data transparency rights are seen as active contributors to a fairer digital environment. As such, they encourage stakeholders to engage with these dimensions and data transparency rights in such a way that their versatile nature, and value within the digital society, can come to full fruition.

5. CONCLUSION

The GDPR provides data subjects with a sound legal framework to obtain transparent and meaningful information regarding the use of their personal data. The general requirement for controllers to provide information to, and communicate with, data subjects in a concise, transparent, intelligible, easily accessible, clear and plain manner implies that meaningfulness must be preserved throughout the processing lifecycle regardless of the system, the level of automation, or the complexity of the operations involved.

The importance of data transparency rights within this context can best be explained in reference to the key functions transparency holds as a general principle underpinning data protection. Transparency holds an intrinsic value as it allows data subjects to make sense of their experiences and interactions within an increasingly complex and datafied physical and digital environment. On an instrumental level, said information can be further harnessed as a means to (re)gain control and challenge power asymmetries.

While data transparency rights serve to realise the intrinsic and instrumental transparency functions, their effectiveness is shaped, and can be evaluated, through the lenses of multiple, interconnected dimensions of which three were discussed as part of this chapter, namely: (1) the data subject's subjective experiences (the data subject dimension), (2) the wider regulatory conditions in which data rights operate (the legal dimension) and (3) the environment in which data transparency rights operate, and in particular, the actors and technologies, including their interrelations, the data subject interacts with (the socio-technical dimension).

One way through which data transparency rights can be further strengthened then, is to recognise the different dimensions that shape their success, and the interplay that exists between these dimensions. Such an analysis can help in locating areas where the further development of data rights is needed. In addition, data transparency rights are instruments that can be exercised in different ways, for different purposes, and with varying degrees of success. We argue that, by focusing on their versatile and polyvalent nature, their value may become better appreciated. In an effort to provide data subjects a stronger basis of empowerment to draw from, the multidimensional analysis offers a twofold purpose: highlighting contextual areas of importance, the dimensions can be used to critically reflect upon how data subject rights are currently perceived and operationalised, whilst also offering a conceptual means through which one can shape their future development in a contextual, goal-oriented and functional manner.

To conclude, in order for data transparency rights to achieve their role as critical safeguards for transparency, empowerment and the mitigation of power asymmetries, it is vital we recognise their multifaceted and versatile nature. The multidimensional framework developed in this chapter helps realising a more nuanced, contextual and goal-oriented approach to vindicate data transparency rights in the digital society.

ACKNOWLEDGEMENTS

The authors would like to thank Oscar Luis Alvarado Rodriguez and Elias Storms for their valuable insight and feedback on co-design strategies.