6 Digital Constitutionalism, Privacy and Data Protection

6.1 Data in the Algorithmic Society

The evolution of the algorithmic society has shed light on the relevance of data in daily life. Algorithms are becoming more pervasive, providing new opportunities for the private sector,[1] and even for the performance of public tasks.[2] The possibilities raised by automated technologies have led to defining data as the raw materials of digital capitalism driving the fourth industrial revolution.[3] These systems are not just drivers of economic growth. Their implementation by public and private actors is increasingly influencing individual decisions without the possibility to understand or control how the processing of personal data affects rights and freedoms.

The organisation and dissemination of information in the digital environment, the profiling of consumers based on credit scores or new techniques in predictive law enforcement are only some examples of the answers which automated decision-making systems can provide and of how such technologies can raise concerns not only from the perspective of individual rights and freedoms but also for democracy. [4] As in the case of freedom of expression, the implementation of algorithms challenges democratic systems due to the lack of transparency

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

[2] Marion Oswald, 'Algorithm-Assisted Decision-making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power' (2018) 376 Philosophical Transaction Royal Society A.

[3] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).

[4] Paul Nemitz, 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) Royal Society Philosophical Transactions A.

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

and accountability in decision-making affecting fundamental rights and freedoms. As Regan underlined, the value of privacy is not just related to the individual dimension and human dignity. It is also a critical safeguard for society.[5]

Orwell's dystopian scenario is not still the rule, but there is an increasing tendency in monitoring and classifying human behaviours in every moment of daily life.[6] From home application to biometric surveillance in public spaces, there are fewer private spaces where individuals can escape from the eyes of public and private actors. Nonetheless, this situation does not concern only the individual private sphere but also the impossibility to scrutinise data collection and use. Individuals tend to adapt their behaviours to a new societal form of surveillance or fear to express themselves, and new information asymmetries do not allow individuals to understand what is happening behind the scenes.[7]

The result is that digital technologies become an instrument for social control. Individuals are increasingly transparent operating in a virtual world which is increasingly opaque. In 2010, Zuckerberg underlined 'The age of privacy is over'.[8] From this perspective, algorithmic technologies are incompatible with data protection which is seen as an obsolete instrument of compliance limiting the datafication of human life for business purposes. This process increasingly makes privacy public while the processing of personal data opaque. These threats do not just involve the private sphere of rights and freedoms but also autonomy and awareness undermined by the lack of transparency and accountability. The case of Cambridge Analytica has been a paradigmatic example of the asymmetry of power in the data field, underlining how the role of microtargeting of voters for electoral purposes challenges fairness and transparency.[9]

[5] Priscilla M. Regan, *Legislating Privacy, Technology, Social Values and Public Policy* 321 (University of North Carolina Press 1995).
[6] George Orwell, *1984* (Penguin Books 2008).
[7] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2018).
[8] Marshall Kirkpatrick, 'Facebook's Zuckerberg Says the Age of Privacy is Over' The New York Times (10 January 2010) www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html?source=post_page accessed 21 November 2021.
[9] Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper Collins 2019).

The large exploitation of data from public and private actors put the protection of personal information under pressure. This is why the reaction of digital constitutionalism does not just involve the right to freedom of expression. The threats of the algorithmic society and digital capitalism affect other two pillars on which liberty and democracy are based in the 'onlife' dimension, in particular the right to privacy and data protection.[10] The latter complements the protection of the former against the threats coming from profiling and, more generally, the computation of human life. Privacy and data protection share a common objective, precisely that of protecting individual autonomy as a precondition to fully participate in a democratic society.

Therefore, data protection in the algorithmic society aims to provide safeguards for individuals while maintaining control of their data. In this sense, data protection represents the 'positive' side of the rights to privacy against interference with the individual freedom to be let alone. Without rules governing the processing of personal data, individuals could not rely on guarantees protecting their privacy and autonomy against the discretionary processing of personal information. Without accountability and transparency safeguards, it is not possible to mitigate the asymmetry of power nor to mitigate the effects of automated decisions on fundamental rights as well as on democratic values.

The constitutional values underpinning privacy and data protection can play a critical role in shaping the exercise of powers in the algorithmic society. While, with respect to content, the primary issue concerns the adoption of procedural safeguards to foster transparency and accountability, the field of data is more mature. Nonetheless, even if the consolidation of the positive dimension of privacy in the right to data protection culminated with the adoption of the GDPR,[11] European data protection law would require further steps forward to address the challenges of the algorithmic society.

Within this framework, this chapter aims to underline how, even in the field of data, European digital constitutionalism provides a normative framework to protect fundamental rights and democratic values while limiting platform power. This process is not based on

[10] Luciano Floridi (ed.), *The Onlife Manifesto Being Human in a Hyperconnected Era* (Springer 2015).

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

introducing new safeguards but providing a teleological interpretation of the GDPR unveiling its constitutional dimension. In other words, protecting privacy and data protection in the European framework would not lead to searching for new rules and instruments to mitigate private powers but interpreting the GDPR under the lens of European digital constitutionalism.

In order to achieve this purpose, the first part of this chapter focuses on the rise and consolidation of data protection in the European framework. This part explains how and to what extent personal data have started to be protected in the algorithmic society. The second part addresses the rise of the big data environment and the constitutional challenges introduced by automated decision-making technologies, thus underlining how the implementation of algorithmic technologies challenges the boundaries of privacy and data protection. The third part focuses on the GDPR underlining the opportunities and challenges of European data protection law concerning artificial intelligence. This part aims to highlight to what extent the system of the GDPR can ensure the protection of the right to privacy and data protection in relation to artificial intelligence technologies. The fourth part underlines the constitutional values underpinning the GDPR to provide a constitutional interpretation of how European data protection, as one of the mature expressions of European digital constitutionalism, can mitigate the rise of unaccountable powers in the algorithmic society.

6.2 From the Right to Be Let Alone . . .

In the field of data, the role of digital constitutionalism in the algorithmic society could be observed by directly focusing on the GDPR. However, such an approach would provide just a limited picture of the underpinning constitutional principles on which the right to data protection is based in Europe. Therefore, understanding which values characterise data protection is critical to provide a constitutional-oriented interpretation of the GDPR. European data protection law is not just the result of regulatory but also historical reasons and constitutional values linked to the evolution of new technologies, precisely automated systems.

The European path towards the constitutional recognition of data protection as a fundamental right began from the evolution of the

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

concept of privacy in the US framework. This right, referred to as 'the right to be let alone' by Warren and Brandeis at the end of the nineteenth century,[12] was conceived as a negative liberty safeguarding the individual's private life against potential external interferences.[13] Also in the European framework, privacy has been conceived as a negative liberty. The Strasbourg Court underlined the right to privacy as the right to live far from publicity,[14] or away from unwarranted attention.[15] This right also extends to online anonymity,[16] thus enabling individuals to live peacefully in the online and offline environment. Nevertheless, the Strasbourg Court has not only underlined the right to privacy as a right to be let alone but also as a condition to development and fulfilment of personality, as well as personal autonomy and identity,[17] intimately connected with the right to human dignity in the European constitutional framework.

However, this historical framework is not enough to explain the reasons triggering the positive evolution of data protection from the negative matrix of privacy. From a merely negative perspective (i.e. the right to be let alone), characterised by predominant liberal imprinting, the right to privacy in Europe has evolved towards a positive dimension consisting of the right to the protection of personal data. This development can be mainly attributed to the increasing role of information to perform public tasks and the evolution of new technologies. It firstly resulted from the increase in data usage and processing, primarily from the progress of the welfare state, the consolidation of new channels of communication (e.g. the telephone) and automated processing techniques like databases.[18] In *Malone* v. *The United Kingdom*, profiling citizens by the public authorities was highlighted as a dangerous trend

[12] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

[13] Daniel J. Solove, 'A Brief History of Information Privacy Law' (2006) Proskauer on Privacy; Alan Westin, *Privacy and Freedom* (Athenum 1967).

[14] *X.* v. *Iceland* (1976) ECHR 7.

[15] *Smirnova* v. *Russia* (2004) 39 EHRR 22.

[16] *Delfi AS* v. *Estonia* (2015).

[17] *Reklos and Davourlis* v. *Greece* (2009) EMLR 290; *Burghartz* v. *Switzerland* (1994) ECHR 22.

[18] Jeffrey A. Meldman, 'Centralized Information Systems and the Legal Right to Privacy' (1969) 52 Marquette Law Review 335; Richard Ruggles, John de J. Pemberton Jr. and Arthur R. Miller, 'Computers, Data Banks, and Individual Privacy' (1968) 53 Minnesota Law Review 211; Arthur R. Miller, 'Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society' (1969) 67 Michigan Law Review 1089.

threatening democratic society.[19] Computing (or information) technologies have introduced new possibilities for storage and organisation of data with lower costs. Nonetheless, this new framework has also introduced new risks related to the automated processing of personal data.[20]

These developments affected the autonomy of individuals. The lack of control and safeguards against the massive collection and processing of data has enabled governmental authorities and private companies to take decisions without explaining which data have been used, for which purposes and duration. In 1983, the German federal constitutional court invalidated a federal law allowing the collection and sharing of census information between national and regional authorities.[21] The case involved the automated collection of personal data by public authorities for the performance of a public task. This decision, known as the *Volkszählungsurteil*, paved the way towards a right to 'informational self-determination' resulting from the constitutional interpretation of enshrining a general right to personality,[22] and the protection of human dignity.[23] This landmark decision highlighted the need to protect personal data from the interferences of automation and its connection with the autonomy and dignity of individuals. The court did not deny that data play a critical role for the development of public policies and the pursuit of public tasks in industrialised countries. At the same time, it shed light on the lack of individual awareness about the processing of personal data for public tasks in the field of tax or social security. This case has provided a first clue of the different characterisation of the right to privacy on the eastern side of the Atlantic and the role of a positive right to data protection aimed to protect the right to self-determination and human dignity.

This European focus on the individual is not by chance. When looking at the eastern side of the Atlantic, different underpinning values have guided the evolution and consolidation of the right to privacy and the

[19] *Malone* v. *the United Kingdom* (1984) 7 EHRR 14.

[20] Council of Europe, 'Convention no. 108/1981 – Explanatory Report' https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 accessed 21 November 2021.

[21] BVerfG 15 December 1983, 1 BvR 209/83, *Volkszählung*.

[22] German Basic Law, Art. 2(1).

[23] Ibid., Art. 1(1). See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review 84.

rise of data protection.[24] As in the case of freedom of expression, the right to privacy in Europe was conceived as a negative freedom but based on different constitutional premises. The European experience has been traumatised by the Second World War where even the right to privacy completely vanished.[25] The increasing amount of data collected for identifying people for creating government records based on data like ethnicity, political ideas and gender is a paradigmatic sample of how such a liberty was compressed. On the other hand, the US has experienced less interferences on privacy and less misuse of personal information, which encouraged a laissez-faire approach based on individual liberty. According to Whitman, Europe would be the dignity side of the Atlantic while the US would represent a model of privacy based on liberty.[26]

The reality is more nuanced, but it cannot be neglected that the grounding values of the right to privacy across the Atlantic are different.[27] This distance is evident indeed when focusing on the evolution of the protection of personal data. In the United States, the protection of privacy is not linked to the individual but to a sectorial approach and the mosaic theory which considers each individual as not relevant per se without the other tiles of the mosaic.[28] In other words, the personalistic characterisation of European data protection law cannot be found on the other side of the Atlantic whose protection is centred on the sectorial and aggregated effects of certain processing of personal information, even if recently privacy and data protection are capturing more attention in the US framework.[29]

It is not by chance that, in that period, some Member States had introduced data protection regulations even before the advent of the Internet,[30] and anticipating the Data Protection Directive. Until 1995, at

[24] Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

[25] Elizabeth Harvey and others (eds.), *Private Life and Privacy in Nazi Germany* (Cambridge University Press 2019).

[26] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) Yale Law Journal 1151.

[27] Paul M. Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy' (2017) 106 Georgetown Law Journal 115.

[28] Orin S. Kerr, 'The Mosaic Theory of the Fourth Amendment' (2012) 111 Michigan Law Review 311.

[29] Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687.

[30] See the *Datenschutzgesetz* adopted on 7 October 1970 in Germany; *Datalagen* adopted on 11 May 1973 in Sweden; Loi n. 78–17 6 January 1978 in France; Data Protection Act 1984 12 July 1984 in UK.

a supranational level, data protection has been primarily addressed within the framework of the Council of Europe through the judicial interpretation of Article 8 of the Convention by the Strasbourg Court.[31]

Together with the Convention, the Council of Europe has specifically focused on the challenges of automation for the right to privacy. In 1968, the Parliamentary Assembly of the Council of Europe proposed to establish a committee of experts to examine whether 'the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods'.[32] This acknowledgement of the role of new data processing techniques is also the reason for the adoption of Convention No. 108 on the protection of individuals with regard to automatic processing of personal data adopted already in 1981.[33] This international instrument was the first to recognise the concerns relating to automated processing when neither the Internet nor artificial intelligence technologies had proven yet that they were the source of new challenges to the protection of personal data. Ensuring the protection of personal data taking account of the increasing flow across frontiers of personal data undergoing automatic processing was the first aim of this document which was subsequently modernised in 2018.[34] As a result, it is possible to underline the role played by automation in founding the constitutional basis for the new fundamental right of data protection whose aim is to protect 'every individual'.[35]

If, at that time, the Council of Europe could be considered the promoter of the constitutional dimension of personal data, this consideration can be extended only partially to the European Union. In this case, the Data Protection Directive regulated the processing of personal data

[31] European Convention on Human Rights (1950). See *Leander* v. *Sweden* (1987) 9 EHRR 433; *Amann* v. *Switzerland* (2000) 30 EHRR 843; *S. and Marper* v. *The United Kingdom* (2008) 48 EHRR 50; *M.M.* v. *UK A no 24029* (2012) ECHR 1906. The ECtHR has justified such approach providing a definition of the Convention as a 'living instrument'. See, also, *Mamatkulov and Askarov* v. *Turkey* (2005).

[32] Parliamentary Assembly of the Council of Europe, 'Recommendation 509 (1968) – Human Rights and Modern Scientific and Technological Developments' https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en accessed 21 November 2021.

[33] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

[34] Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

[35] Ibid., Art. 1.

only in 1995 and before the adoption of the Charter of Nice in 2000,[36] which recognised data protection as a fundamental right,[37] albeit without any binding character until the entry into force of the Lisbon Treaty in 2009.[38] As already underlined in Chapter 2, it would be enough to look at the Recitals of the Data Protection Directive highlighting the functional (and non-fundamental) nature of the protection of personal data for the consolidation and proper functioning of the single market,[39] and, consequently, as an instrument to guarantee the fundamental freedoms of the Union.[40] This scenario based on the prevalence of the economic-functional dimension of the protection of personal data, the recognition of the binding nature of the Charter and the inclusion in EU primary law have contributed to codifying the constitutional dimension of the right to data protection in the Union.[41] This change of paradigm has led the ECJ to extend the boundaries of protection of these fundamental rights, thus triggering a positive regulatory outcome with the adoption of the GDPR.

Data protection in the European framework constitutes a relatively new right developed as a response to technological evolution.[42] European data protection law is an example of the shift from a mere negative liberty (i.e. privacy) to a positive right (i.e. data protection) to face the threats coming from the unaccountable exercise of powers through the processing of personal data. The advent of the Internet has not only lowered this cost but has also increased the speed for transferring large sets of information and connecting single nodes into a network for sharing data.[43] Thanks to the evolution of data management systems, the public and private sector benefited from

[36] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.
[37] Ibid., Art. 8.
[38] Consolidated version of the Treaty on European Union (2012) OJ C 326/13, Art. 6.
[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31.
[40] Data Protection Directive (n. 39). According Recital 3: 'Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded'.
[41] Hielke Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU* (Springer 2016).
[42] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015). Gonzalez Fuster (n. 24).
[43] Helen Nissenbaum, 'Protecting Privacy in a Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

the new possibilities of the data-driven economy. The broad protection of privacy and personal data in Europe limits the possibility to develop and implement technologies escaping transparency and accountability. It is not by chance that the right to privacy in Europe has been defined as the US First Amendment.[44] Besides, as observed by the ECJ, data protection needs to be ensured, primarily when automated processing is involved, thus recognising a specific threat coming from automation and, *a fortiori*, on artificial intelligence technologies.[45]

If the right to privacy was enough to meet the interests of individual protection against public interferences, in the algorithmic society, the widespread processing of personal data through automated means has meant that it is no longer enough to protect only the negative dimension of this fundamental right. It has been the role of digital technologies to trigger the rise of data protection as the positive side of the right to privacy and as a new and autonomous fundamental right in the European framework. Therefore, the next section focuses on examining the rise of Big Data analytics to understand the limits of European data protection law given the lack of an interpretative lens unveiling its constitutional dimension.

6.3 … To Privacy and Data Protection in the Age of Big Data

'Data is the new oil'.[46] This is one of the most common expressions to describe the role of data in the information society where algorithmic processing contributes to the extraction and creation of value. Nonetheless, data do not exactly fit within this definition, precisely because of their immateriality. Unlike oil, data can be reused multiple times, for different purposes and in non-rivalrous ways, without being consumed or losing their value. While oil is refined and consumed, the use of data is potentially perpetual.

[44] Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25(2) European Law Journal 140.

[45] Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (2014) 54 and 55; Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner* (2015), 91. See, also, as regards Article 8 ECHR, *S. and Marper* v. *the United Kingdom* (2008) 103, and *M. K.* v. *France* (2013), 35.

[46] 'The World's Most Valuable Resource is no Longer Oil, but Data' The Economist (6 May 2017) www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data accessed 21 November 2021.

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

The idea of data as oil however could be considered accurate when looking at the ability of data to generate value. Like oil for the industrial economy, the processing of a vast amount of data becomes a primary and endless source of values in the algorithmic society. As with other expressions in the field of digital technologies, the term 'Big Data' has become a metaphor.[47] In 2011, the term was used by the McKinsey Global Institute, which defined Big Data as data sets whose size exceeds a database's ability to acquire, store, manage and analyse data and information.[48]

At the beginning of this century, Laney's three-dimensional model on data management based on Volume, Variety and Velocity already anticipated the premises of Big Data analytics.[49] These three Vs were developed in the context of e-commerce to generally describe the increase in the amount of data deriving from homogeneous and heterogeneous sources such as, for example, online accounts and sensors (i.e. Volume). Along with an exponential increase in the quantity of data, the sources have multiplied. If, on the one hand, the increase in volume constitutes one of the primary characteristics, on the other hand, the heterogeneity of the sources and types of data constitutes a fundamental element to fully understand the phenomenon of Big Data (i.e. Variety). In the past, the processing of data was characterised by structured data, namely information stored in databases organised according to rigid schemes. The development of new analytics techniques has allowed the exploitation of the so-called unstructured data or data that is not placed under any pattern or scheme.[50] The third element of growth is the rapid creation and sharing of data (i.e. Velocity). This model was then enriched by (at least) two other characteristics, namely Veracity and Value,[51] even if these elements reflect a different logic from Laney's model based on incremental growth.

[47] Cornelius Puschmann and Jean Burgess, 'Big Data, Big Questions. Metaphors of Big Data' (2014) 8 International Journal of Communication 1690.

[48] James Manyika and others, 'Big Data: The Next Frontier for Innovation, Competition, and Productivity' McKinsey Global Institute (2011) www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation accessed 21 November 2021.

[49] Doug Laney, '3D Data Management: Controlling Data Volume, Velocity and Variety' (2001) Application Delivery Strategies.

[50] Rob Kitchin and Tracey P. Lauriault, 'Small Data, Data Infrastructures and Big Data' (2014) 80(4) GeoJournal 463.

[51] Chun-Wei Tsai and others, 'Big Data Analytics: A Survey' (2015) 2 Journal of Big Data 21.

When looking at these characteristics in the context of the protection of privacy and personal data, the techniques used for processing purposes constitute a critical factor in the processing of personal data. It is no coincidence that Big Data analytics have been defined as 'the storage and analysis of large and or complex data sets using a series of techniques including, but not limited to: NoSQL, Map Reduce and machine learning'.[52] The mix of these techniques is used for general value or to derive new information from apparently heterogeneous data. From traditional forms of data processing based on deterministic rules, Big Data analytics rely on new forms of processing using unstructured or semi-structured data such as multimedia content and social media accounts.[53] Content, blog posts, comments or accounts leave online traces revealing large parts of personal information. This issue is also relevant when considering the information collected after visiting webpages (e.g., cookies) or using online applications which track users passively.

Therefore, the combination between quantitative and qualitative data makes Big Data a 'new generation of technologies and architectures, designed to economically separate value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and analysis'.[54] This definition can complement the idea of Boyd and Crawford who identified three criteria: technology, analysis and mythology.[55] By technology, they mean the mix of computing power and algorithmic methods capable of leading to the collection and analysis of large clusters of data. The analysis phase consists of identifying and predicting models that could have economic, social or legal effects. Mythology refers to the belief that new levels of forecast and knowledge can be obtained using these processing techniques. In light of these considerations, it is possible to define the phenomenon of Big Data as the collection and analysis of a large volume of structured and unstructured data through computational skills or algorithms to discover

[52] John S. Ward and Adam Barker, 'Undefined By Data: A Survey of Big Data Definitions' ArXiv http://arxiv.org/abs/1309.5821 accessed 21 November 2021.

[53] Richard Cumbley and Peter Church, 'Is Big Data Creepy?' (2013) 29 Computer Law and Security Review 601.

[54] Priyank Jain, Manasi Gyanchandani and Nilai Khare, 'Big Data Privacy: A Technological Perspective and Review' (2016) 3 Journal of Big Data.

[55] Danah Boyd and Kate Crawford, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2015) 15 Information Communication and Society 662.

models and correlations that can lead to predictive analysis or automated decisions.

The relevance of the processing explains why attention has been paid to the phase of analytics, namely the processing techniques (e.g. data mining) to define models or find correlations between structured and unstructured data sets.[56] The scope of this processing is different from the traditional search for information based on causal relationships. The implementation of algorithms in the phase of analytics has moved the focus from causality to probabilities and correlations. Traditional systems of processing are not enough to deal with the vast amount of data, thus encouraging the implementation of statistical methods. This shift from causality to probability is not neutral but raises concerns about the reliance on the outcome of these technologies.

This new framework has captured the European attention due to the challenges in protecting privacy and personal data. The WP29 underlined the growing expansion both in the availability and in the automated use of data analysed through automated systems. As underlined, 'Big data can be used to identify more general trends and correlations but ... big data may also pose significant risks for the protection of personal data and the right to privacy'.[57] The European Data Protection Supervisor has also intervened in this field by underlining how modern data collection and analytics techniques represent challenges for the protection of privacy and personal data.[58] Even the Council of Europe has adopted a definition that highlights the relevance of the new methods of data processing since, as regards the protection of privacy,

[56] According to the European Union Agency for Cybersecurity (ENISA), Big Data analytics refers to 'the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours'. Giuseppe D'Acquisto and others, 'Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics', ENISA (December 2015) www.enisa.europa.eu/publications/big-data-protection accessed 21 November 2021.

[57] Working Party Article 29, 'Opinion 03/2013 on Purpose Limitation' (April 2013) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf accessed 21 November 2021.

[58] According to the EDPS, Big Data refers to 'the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data'. European Data Protection Supervisor, 'Opinion 7/2015, Meeting the challenges of Big Data' (November 2015) https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf accessed 21 November 2021.

the focal issues consist not just of the quantity and variety of the data processed but especially their analysis leading to predictive and decisional results.[59] In other words, the processing phase is the critical moment for the purposes of privacy and the protection of personal data since it does not only influence the collection of data but also the predictive and decision-making output. The phase of analytics can be considered, on the one hand, the step from which value is extracted from the analysis of different categories of data. On the other hand, it is also the phase leading to the algorithmic output producing the most relevant effect for individuals and society.

This challenge is particularly relevant when considering that public and private actors increasingly rely on algorithms for decision-making and predictive models. Although data constitute a crucial economic asset in the algorithmic society due to the value generated by its processing and marketing, at the same time, data can be closely linked to the individual identity and private sphere, thus leading to discrimination and interferences with the right to privacy. In other words, on the one hand, Big Data analytics can stimulate innovation of digital services by ensuring private economic initiatives and the free flow of information. On the other hand, these technologies can lead to disproportionate interferences with fundamental rights and democratic values while contributing to the consolidation of unaccountable powers.

6.4 The Constitutional Challenges of Big Data

The constitutional dimension of Big Data is hidden behind the opacity of algorithmic technologies. At first glance, algorithms could be considered as neutral and independent systems capable of producing models and answers useful for dealing with social changes and market dynamics. From a technical point of view, algorithms are mathematical methods expressing results within a limited amount of space and time and in a defined formal language, transforming inputs, consisting of data, into outputs based on a specified calculation process. Nonetheless, from a social point of view, these technologies constitute decision-making processes designed by programmers and developers. The human contribution in the development of these technologies leads to

[59] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD (2017)01.

the translation of personal interests and values into algorithmic processes.[60] In other words, algorithms express results which, although determined by their code, constitute subjective determinations provided by automated systems. This underlines how algorithms are not the exclusive source of challenges in the digital age. Behind these technologies, there are actors developing and implementing these systems to pursue their public and private interests.

In this scenario, if algorithms are tools to extract value from data, then, moving to a social perspective, these technologies constitute automated decision-making processes influencing the rights of individuals and society at large. The processing of a vast amount of data allows to obtain information about the behaviours, preferences and lifestyles of data subjects.[61] The implementation of automated decision-making, especially based on machine-learning techniques, raises challenges not only for privacy and data protection but also for the potential discriminatory and biased results coming from inferential analytics.[62]

If this scenario may not look less problematic at first glance, however, the same processing acquires a different value when the categorisation of the individual in a group rather than in another one leads to a decision affecting individuals' rights.[63] Profiling and automated decisions are processes whose implicit purpose is to divide groups of individuals into different categories based on common characteristics and make decisions based on the membership of a specific group, raising question beyond data protection.[64] Besides, profiling and automated decision-making do not focus only on the individual, but also on

[60] Philip A. E. Brey and Johnny Soraker, *Philosophy of Computing and Information Technology* (Elsevier 2009); Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press 1988).

[61] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1; Tal Zarsky, 'Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375; Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2(2) Journal of Information Rights, Policy and Practice https://jirpp.winchesteruniversitypress.org/articles/abstract/10.21039/irpandp.v2i2.45/ accessed 21 November 2021.

[62] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

[63] Brent D. Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303.

[64] Raphaël Xenidis, 'Tuning EU equality law to algorithmic discrimination: Three pathways to resilience' (2021) 27(6) Maastricht Journal of European and Comparative Law 736.

clusters or groups based on common characteristics.[65] This automatic classification can lead to discrimination and serious effects on individual fundamental rights and freedoms.[66] The case of algorithmic discrimination by search engines can be considered a paradigmatic example of the implications of these technologies across society.[67]

This trend is increasingly relevant in the algorithmic society where the role of (personal) data plays a critical role in the public and private sector. As underlined by the GDPR, technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their business goals. Natural persons increasingly make personal information available publicly and globally.[68]

Everything is transforming into digital data. At the beginning of this century, the dematerialisation and digitisation of different products have contributed to increasing the amount of information flowing online. Music, videos and texts are nothing else than data. In the algorithmic society, the dematerialisation concerns the individual and its identity which is increasingly subject to datafication. In this case, data controllers can obtain even intimate information concerning private life.

These considerations only provide some examples of why constitutional law is relevant in the case of algorithmic systems processing personal data. Big Data analytics provide opportunities for data analysis leading to insights into social, economic or political matters. At the same time, the probabilistic and statistic approach makes these outcomes problematic since correlation does not per se imply causation. If correlation overcomes causation, legal systems are exposed to risks coming from determinations whose degree of error or inaccuracy is

[65] Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor and others (eds.), *Group Privacy* (Springer 2017).

[66] 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; Talia B. Gillis and Jann L. Spiess, 'Big Data and Discrimination' (2019) 86 The University of Chicago Law Review 459; Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6(2) Big Data & Society https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805 accessed 21 November 2021.

[67] Safiya U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018).

[68] GDPR (n. 11), Recital 6.

the natural result of a probabilistic logic. Within this framework, data protection plays a critical role in the algorithmic society since the datafication of society makes this fundamental right functional (or even necessary) to protect the right to privacy. Without ensuring that data are processed according to safeguards based on transparency and accountability, it is not possible to protect the unlawful processing of personal data and mitigate the interferences with the right to privacy. In other words, artificial intelligence technologies underline the critical role of data protection as a shield of individual self-determination and dignity against the new challenges raised by digital capitalism.[69]

Furthermore, the role of data protection in the algorithmic society acquires a critical position not only to protect individual privacy but also as a safeguard for democratic values. The effective protection of privacy allows people to exercise their individual autonomy. In a democratic society, protecting privacy enables citizens to develop their beliefs, freely exchange opinions and express their identities. In order to promote autonomy and self-determination, it is critical that individuals can control their identity and how their personal information is processed.[70] One of the primary challenges for democracy comes from regimes of public and private surveillance which, based on the processing of personal data, can lead to different profiling or targeting of users. This process can affect not only the right to privacy but also freedom of expression, with clear effects on democratic values. Therefore, liberal arguments based on 'anything to hide' fails to represent how people adapt their behaviours when they are observed or identifiable.[71]

Informational privacy is therefore critical for democracy,[72] but could not be enough without data protection law. Data protection does not only protect individuals against surveillance but also fosters transparency and accountability to mitigate the asymmetries of powers that threaten democratic values. The processing of vast amounts of data would lead to clear interferences with the possibility to understand how personal data are processed and according to which criteria. This

[69] Anne de Hing, 'Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation' (2018) 19(5) German Law Journal 1270.
[70] Charles Fried, 'Privacy: A Moral Analysis' (1968) 77 Yale Law Journal 475.
[71] Daniel Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press 2013).
[72] Volker Boehme-Neßler, 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection' (2016) 6(3) International Data Privacy Law 222.

is why data protection is a necessary piece of the democratic puzzle in the algorithmic society.[73] It allows citizens to make informed decisions (i.e. decisional privacy),[74] while protecting their private sphere. As a result, a democratic digital society would fail not only without privacy but also without data protection.

Besides, the increasing reliance on automated decision-making could lead democratic values to lose their attraction. Zuboff has described some examples of how big tech corporations have built a surveillance capitalism based on the users' addiction to friendly technologies and under the logic of accumulation.[75] The neoliberal charm using efficiency and innovation as a justification to massively implement automated decision-making technologies could lead to a process of dehumanisation where the logic of the market guide not only business interests but imbues even the activities of public authorities. The mix of public and private values is a primary challenge for protecting the human dimension of the algorithmic society.

Within this framework, data protection plays a primary role to foster transparency and accountability against opaque processing, thus promoting the right to privacy and self-determination as pillars for democracy while limiting powers. Although, at first glance, the GPDR, as a milestone of European digital constitutionalism, aims to foster the protection of personal data in the Union, the application of data protection rules to the algorithmic environment is far from being straightforward. The implementation of artificial intelligence promises to provide new phases of growth for the internal market and foster fundamental freedoms while, at the same time, the massive processing of personal data through algorithmic technologies questions the basic foundation of data protection law and challenges the protection of fundamental rights and freedoms. This is primarily because there is an intimate connection between (constitutional) law and technology in this case due to the relevance of (personal) data in the algorithmic society.[76]

[73] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds.), *Reinventing Data Protection?* 45 (Springer 2009).

[74] Neil M. Richards, 'The Information Privacy Law Project' (2006) 94 Georgetown Law Journal 1087.

[75] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75.

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

As underlined by the next subsection, the implementation of algorithmic technologies highly challenges the boundaries of European data protection law. This issue requires the examination of the relationship between the GDPR and Big Data analytics, particularly focusing on the notion of personal data, the general principles of the GDPR and automated decision-making processes.

6.4.1 The Blurring Boundaries of Personal Data

The scope of application of the GDPR is firmly dependent on the notion of personal data. As already observed, such a personalistic approach characterises the European legal framework of protection in the field of data. In the algorithmic society, the economic value of Big Data comes from the processing of personal and non-personal data. Therefore, in order to trigger the machine of European data protection law, it is necessary to understand when the link between information and individuals leads to defining data as 'personal'.

The GDPR only applies to the processing of 'personal data' as 'any information concerning an identified or identifiable natural person'.[77] While the notion of 'identified natural person' does not raise particular concerns for defining personal data, the notion of identifiability deserves more attention, especially when artificial intelligence technologies are involved. The GDPR provides a comprehensive approach concerning the identifiability of the data subject which can be identified by 'all means ... which the data controller or a third party can reasonably use to identify said natural person directly or indirectly'.[78] The assessment concerning the reasonableness of these means should be based on objective factors 'including the costs and the time required for identification, taking into account both the technologies available at the time of treatment and the technological developments'.[79]

Within this framework, the ECJ has extensively interpreted the notion of personal data extending its boundaries also to information apparently outside this definition. For instance, in *YS*,[80] the ECJ clarified that the data relating to an applicant for a residence permit contained in an administrative document, and the data in the legal analysis contained

[77] GDPR (n. 11), Art. 4(1)(1).
[78] Ibid., Recital 26.
[79] Working Party Article 29, 'Opinion 4/2007 on the Concept of Personal Data' (June 2007) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf accessed 21 November 2021.
[80] Joined Cases C-141/12 and C-372/12, *YS* v. *Minister voor Immigratie* (2014).

in that document, are personal data, while the analysis per se cannot be considered within this notion. Likewise, in *Digital Rights Ireland*,[81] the ECJ recognised the relevance of metadata as personal data since they could make it possible 'to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place'.[82] Therefore, the ECJ extended the notion of personal data considering also the risk of identification deriving from the processing of certain information.

The same approach was adopted in *Breyer*.[83] The dispute concerned the processing and storing of dynamic IP addresses of visitors to institutional websites by the German federal institutions to prevent cyber-attacks. The domestic court asked the ECJ whether the notion of personal data also included an IP address which an online media service provider stores if a third party (an access provider) has the additional knowledge required to identify the data subject. In *Scarlet*,[84] the ECJ had already found that static IP addresses should be considered personal data since they allow users to be identified. In this case, the attention is on dynamic IP addresses that cannot independently reveal the identity of a subject as they are provisional and assigned to each Internet connection and replaced in the event of other accesses. Therefore, the primary question focused on understanding whether the German administration, as the provider of the website, was in possession of additional information that would allow the identification of the user. The ECJ identified such means in the legal instruments allowing the service provider to contact, precisely in case of cyber-attacks, the competent authority, so that the latter takes the necessary steps to obtain this information from the former to initiate criminal proceedings. As a result, firstly, this case shows that, for the purpose of the notion of personal data, it is not necessary that information allows the identification of the data subject per se. Secondly, the information allowing identification could not be in the possession of a single entity.

The ECJ addressed another case enlarging the scope of the notion of personal data in *Novak*.[85] The case concerned the Irish personal data authority's refusal to guarantee access to the corrected copy of

[81] Cases C-293/12 and C-594/12 (n. 45).
[82] Ibid., 26.
[83] Case C-582/14, *Patrick Breyer* v. *Bundesrepublik Deutschland* (2016).
[84] Case C-70/10, *Scarlet Extended SA* v. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) ECR I-11959.
[85] Case C-434/16, *Peter Nowak* v. *Data Protection Commissioner* (2017).

an examination test due to the fact that the information contained therein did not constitute personal data. After reiterating that the notion of personal data includes any information concerning an identified or identifiable natural person, the ECJ observed that, in order to answer the question raised by the national court, it is necessary to verify whether the written answers provided by the candidate during the examination and any notes by the examiner relating to them constitute information falling within the notion of personal data. The ECJ observed that the content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes and judgment as well as graphological information. The collection of these responses also has the function of assessing the candidate's professional skills and their suitability to exercise the profession in question. Finally, the use of such information, which translates into the success or failure of the candidate for the exam in question, can have an effect on their rights and interests, as it can determine or influence, for example, their ability to access the desired profession or job. Likewise, with regard to the examiner's corrections, the content of these annotations reflects the examiner's opinion or evaluation on the candidate's individual performance during the examination, and, precisely, on their knowledge and skills in the field in question. Together with *Breyer*, this case shows an extensive approach to the notion of personal data with the result that it is not possible to foresee in any case when information should be considered 'personal' but it is necessary to examine the context through a case-by-case analysis.

In the algorithmic society, this overall picture would lead to consider *a fortiori* how the dichotomy between personal and non-personal data looks less meaningful. Even if the processing of personal data through artificial intelligence technologies does not always involve personal data such as, for example, climatic and meteorological data, the potentiality of artificial intelligence technologies to find correlation through a mix of related and unrelated as well as personal and non-personal data, broadens the cases in which the scope of application of the GDPR covers the processing of information which would not fall within the notion of personal data at first glance. For instance, big data analytics aims to identify correlations based on originally unrelated data.[86] It is

[86] GDPR (n. 11), Recital 30. According to this Recital: 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when

the processing of different types of data that could lead to discovering or redefining data or information as personal.[87] Therefore, it could be impossible to find information that cannot be potentially transformed into personal data,[88] precisely because the economic value of Big Data encourage to process vast amounts of personal and non-personal data.

This consideration could be extended even to the process of anonymisation of personal data. The GDPR does not apply to anonymous data or information that does not refer to an identified or identifiable natural person or to personal data made sufficiently anonymous to prevent or disallow the identification of the data subject. Consequently, anonymised data would not fall within the scope of application of the GDPR. However, it could be easy to define the cases in which the anonymisation process is not reversible or apparently anonymous data are instead personal when mixed with other information. Therefore, there is no single definition of anonymous data, but this notion should be considered in the framework in which the data controller operates, taking into account 'all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.[89]

The primary criterion to assess whether data are anonymous comes from a mix of factors and refers to the reasonable usability of the available means to reverse the process of anonymisation referring precisely to 'all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'.[90] According to Finck and Pallas, this complexity is linked both to technical and legal factors. On the one hand, '[f]rom a technical perspective, the increasing availability of data points as well as the continuing sophistication of data analysis algorithms and performant hardware makes it easier to link datasets and infer personal information from ostensibly non-personal data'. On the other hand, '[f]rom a legal

combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them'.

87 Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814.

88 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.

89 GDPR (n. 11), Recital 26.

90 Ibid.

perspective, it is at present not obvious what the correct legal test is that should be applied to categorise data under the GDPR.[91]

Therefore, even data that would lead to the identification of individuals could be considered anonymous, due to the absence of reasonable means to obtain personal data from that information. Nonetheless, as underlined by Stalla-Bourdillon and Knight, the approach to anonymisation would be idealistic and impractical.[92] This is because the phase of analytics plays a crucial role in the anonymisation of personal data. It is possible to observe how the quantity and quality of elements identifying personal data influence the number of resources needed for anonymisation. There is a point where the resources available no longer allow the identification due to the number of data to be anonymised. The anonymisation process is effective when it can prevent anyone using reasonable means from obtaining personal data from anonymised data consisting of irreversible de-identification.[93] According to the WP29, 'the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, as permanent as erasure, i.e. making it impossible to process personal data'.[94] The concept of anonymous data still creates 'the illusion of a definitive and permanent contour that clearly delineates the scope of data protection laws'.[95] Anonymising data could not mean that we are not dealing with personal data any longer. Even when the data controller makes it almost impossible to identify the data subject, evidence shows that the risk of re-identification is concrete.[96] The WP29 has already underlined that the advance of new technologies makes anonymisation increasingly difficult to achieve. Researchers

[91] Michele Finck and Frank Pallas, 'They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10(1) International Data Privacy Law 11, 11.

[92] Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data' (2017) 34 Wisconsin International Law Journal 284.

[93] Working Party Article 29, 'Opinion 05/2014 on Anonymisation Techniques' (2014), 6 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf accessed 21 November 2021.

[94] Ibid., 6.

[95] Khaled El Emam and Cecilia A. lvarez, 'A Critical Appraisal of the Article Working Party Opinion 05/2014 on Data Anonymization Techniques' (2015) 5 International Data Privacy Law 73, 81–2.

[96] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105.

have underlined the fallacies of anonymisation in different fields,[97] especially when Big Data analytics are involved.[98]

Furthermore, even when focusing on pseudonymisation, the GDPR still applies.[99] Pseudonymisation consists of 'the processing of personal data so that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures intended to ensure that such personal data is not attributed to an identified or identifiable natural person'.[100] The GDPR explicitly promotes the use of this technique as a risk-management measure but not as an exception to its scope of application. Unlike anonymisation, the data controller can reverse pseudonymised data, and this is why this information falls within the scope of personal data.

Pseudonymisation consists just of the replacement of data with equally univocal, but not immediately, intelligible information. Therefore, on the one hand, as long as data can be considered anonymous, this information can be processed freely by using Big Data analytics techniques, provided that, as already underlined, the processing does not lead to the identification of the data subject. On the other hand, in the case of pseudonymisation, the discipline of the GDPR applies and, as a result, the data controller is responsible for assessing the risks of this processing and relying on the appropriate legal basis. Furthermore, even if it cannot be excluded that, in some cases, pseudonymised data could be close to the notion of anonymity, they could fall under the processing of the GDPR allowing the data controller not to maintain, acquire or process additional information if the purposes for which a controller processes personal data do not or do no longer require the identification of data subjects.[101]

[97] Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of Personally Identifiable Information' (2010) 53 Communications of the ACM 24, 26; Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069.

[98] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCL Law Review 1701.

[99] Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review 222.

[100] GDRP (n. 11), Art. 2(5).

[101] Ibid., Art. 11. In this case, the data controller is not required to comply with Arts. 15–20 GDPR unless the data subject provides additional information enabling their identification for the purposes of exercising these rights.

Therefore, on the one hand, the GDPR would increase the protection of data subjects by extending the scope of the notion of personal data. The more the notion of personal data is broadly interpreted, the more the processing of data through artificial intelligence technologies falls under data protection laws and, therefore, the processing of information through these technologies is subject to the GDPR's safeguards. However, the impossibility to foresee when this technique could lead to the reidentification of data undermines legal certainty, thus constituting a brake to the development of digital technologies in the internal market.

6.4.2 Clashing General Principles

The implementation of artificial intelligence technologies to process personal information does not just contribute to blurring the gap between non-personal and personal data but also to broadly challenge the general principles governing the GDPR. Once information falls within the category of personal data, the relationship between the GDPR and algorithmic processing is far from being exhausted. The challenges concern not only the scope of application of European data protection law but also its founding principles. It would be enough to look at the Charter underlining that 'data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[102] Together with other grounding values, the GDPR has introduced these principles representing the expression of the constitutional dimension of privacy and data protection as fundamental rights of the Union.

The GDPR's general principles can be considered the horizontal translation of constitutional values guiding data controllers when ensuring the compliance with data protection rules and the protection of the data subject's rights. General principles play a crucial role in avoiding that the processing of personal data leads to serious interference with the data subjects' fundamental rights. At the same time, they constitute axiological limits to the exercise of powers based on the discretionary processing of personal data.

Generally, the analysis of large quantities of data through opaque processing leading to outputs that are not always predictable are just some elements to consider when assessing the compatibility of Big Data analytics with the general principles of European data protection law.

[102] Charter (n. 36), Art. 8(2).

Such a multifaceted analysis of data for multiple purposes raises serious concerns about, but not limited to, the principles of lawfulness, fairness and transparency. These principles require natural persons to be made 'aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing'.[103] The obligations for the data controller to inform data subjects about the processing of their personal data,[104] or the legal basis for processing personal data, are just two examples expressing (or implementing) the general principles.[105] As observed by Gutwirth and De Hert, while the right to privacy is an instrument of opacity for the protection of the individual, data protection plays the role of a transparency tool.[106]

These principles are challenged by algorithmic processings whose decision-making processes are often opaque.[107] These techniques do not always allow to explain to data subjects the consequences of processing their personal data through such systems. For example, Big Data analytics often involve the re-use of data and lead to the creation of other information through inferences.[108] Therefore, it would not always be possible to predict from the beginning all the types of data processed and potential uses.[109] Therefore, the process of mandatory disclosure required by the GDPR would de facto fail before the characteristics of these technologies. It is no coincidence that Richard and King have defined this situation as a 'transparency paradox'.[110] On the one hand, Big Data analytics promise new levels of knowledge by defining models and predictions. On the other, the mechanisms by which these

[103] GDPR (n. 11), Recital 39.
[104] Ibid., Arts. 14–15.
[105] Ibid., Arts. 6, 9.
[106] Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional States' in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen* 271 (Springer 2008).
[107] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015); Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11(2) Ethics and Information Technology 105; Tal Zarsky, 'Transparent Predictions' (2013) 4 University of Illinois Law Review 1507.
[108] Sandra Wachter and Brent D. 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.
[109] Ira S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74.
[110] Neil M. Richards and Jonathan H. King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41.

systems reach a new degree of knowledge are obscure. In other words, the price to access more knowledge is accepting a certain degree of data ignorance.

The information asymmetry between the data subject and data controller leads to questioning not only the principle of transparency but also those of lawfulness and fairness. The lack of transparency in the processing may not always allow the data subject to express a valid consent.[111] Artificial intelligence technologies challenge how data subjects express their free and informed consent. In this situation, where the data controller cannot explain the potential use of data transparently, the data subject is not aware of the risks when giving their consent to access products and services. Such information asymmetry is even more problematic when the data subject needs, for example, to access public services which are provided by a data controller or the data controller in a position of monopoly or oligopoly. According to the GDPR, the legal basis of consent should not be valid for processing personal data where there is a clear imbalance between the data subject and the data controller.[112]

Besides, the principle of lawfulness is undermined not only by the low level of transparency in the field of artificial intelligence but also by how information about the processing of personal data is shared with data subjects through privacy policies. This issue is not only relating to the use of long and complex explanations about the processing of personal data undermining de facto the possibility for data subjects to really understand how their personal data are used and for which purposes.[113] Another primary issue concerns the spread of daily life applications (i.e. Internet of Things) collecting personal data in public and private places without the awareness of data subjects.[114] The strict rules to obtain consent and the burden of

[111] Alessandro Mantelero, 'The Future of Consumer Data Protection in the EU Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30(6) Computer Law & Security Review 643.

[112] GDPR (n. 11), Recital 43.

[113] Aleecia M. Mcdonald and Lorrie F. Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 543.

[114] Carsten Maple, 'Security and Privacy in Internet of Things' (2017) 2 Journal of Cyber Policy 155; Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 85; Rolf H. Weber, 'Internet of Things – New Security and Privacy Challenges' (2010) 26 (1) Computer Law & Security Review 23.

proof can prevent discretionary determinations over personal data but also encourage data controllers to rely on other legal bases beyond consent.[115]

This trend could be problematic for the principle of lawfulness also because the legal bases for the processing of personal data do not apply when the data controller processes particular categories of data, namely 'those personal data that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical, or union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sexual life or sexual orientation of the person'.[116] As already observed, the analysis of a vast amount of data from heterogeneous datasets can lead to the discovering of new data (i.e. inferences) which could require a different legal basis to process them.[117]

In the algorithmic society, the rationale behind the distinction between 'ordinary' and 'particular' categories of data tends to be nullified by the way in which the data are processed for at least two reasons. Firstly, Big Data analytics are based on a high volume of structured and unstructured data, which usually do not rely on the distinction between categories of data. Secondly, data on health, race or sexual orientation can be obtained from the processing of unstructured data. For example, the content of a social network account can reveal health or racial origin data that inevitably become part of the analysis process that leads to profiling or an automated decision. In other words, even non-particular categories of data can constitute a vehicle for the deduction of information of a particular nature. As noted by Zarsky, 'the rise of big data substantially undermines the logic and utility of applying a separate and expansive legal regime to special categories'.[118]

Such a consideration also shows how artificial intelligence technologies challenge the principle of purpose limitation, precisely due to the multiple and unpredictable re-use of data.[119] It would not be by chance

[115] GDPR (n. 11), Recital 42.
[116] Ibid., Art. 9.
[117] Wachter and Mittelstadt (n. 108).
[118] Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 1014.
[119] Nikolaus Forgó and others, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales and others (eds.), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation* 17 (Springer 2017).

if the WP29 focused on the need to respect this principle in the field of Big Data by ensuring that the purposes for which the data is processed can be known or foreseen by the data subjects.[120] In order to comply with the principle of purpose limitation, it is necessary to inform the data subject of the processings whose purposes differ from the initial ones at the time of data collection and analysis. Therefore, the aim of this principle is to protect data subjects against the unforeseeable extension of processing purposes. The general use of Big Data analytics implies that data is not just held and used by a certain and predetermined number of third parties for a specific purpose. On the contrary, as observed by Mittelstadt, data 'travels with the person between systems and affects future opportunities and treatment at the hands of others'.[121]

Besides, the relevance of the principle of purpose limitation deserves to be examined not only by looking at the protection of data subjects' rights but also by considering the effects that such a principle can produce on the internal market. It could constitute a barrier to the development of monopolies and dominant situations in the context of data analysis by limiting the possibility for data controllers to use data for any contingent purpose. Nevertheless, as Hildebrandt observed, a narrow interpretation of this principle could limit the potentialities of analytics which, usually, rely on creating models and previsions based on unrelated data and purposes.[122] The principle of purpose limitation can indeed constitute a barrier to data-driven innovation, especially for data sharing. However, what is defined as 'purpose limitation' could be more precisely described as 'non-incompatibility'.[123] Since it is not possible in some cases to foresee all the potential uses, the principle of purpose limitation would apply only in relation to that processing which is incompatible with those disclosed to the data subject.

Nonetheless, the challenges to the principles of transparency, lawfulness and fairness do not exhaust the concerns about the relationship between algorithmic technologies and the GDPR's general principles.

[120] Working Party Article 29, 'Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of their Personal Data in the EU' (2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf accessed 21 November 2021.

[121] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30(4) Philosophy and Technology 475, 482.

[122] Mireille Hildebrandt, 'Slaves to Big Data. Or Are We?' (2013) 17 IDP Revista de Internet Derecho y Política 7.

[123] Working Party Article 29 (n. 57).

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

The collection and analysis of vast amounts of data can affect the principle of data minimisation. Bygrave has described this principle as an instrument to ensure proportionality and necessity without exceeding the quantity of data to be processed.[124] Unlike the processing of data through analogical means, new automated processing techniques allow extracting value even from apparently unrelated data. This feature has been facilitated by the possibility of storing and analysing increasing amounts of data according to the so-called 'N = all' model according to which the collection and analysis of information are not based just on relevant data but on the whole.[125] The processing and accumulation of a vast amount of data also threaten the principles of integrity and confidentiality due to the increasing risks in handling large volumes of information to be managed.[126] The more data are processed and stored, the more the risk of facing serious data breaches will be amplified. Likewise, the trend towards data accumulation could also clash with the principle of data retention and security.[127] Dealing with large amounts of data processed for multiple purposes could make retention policies complex to implement and security measures subject to increasing layers of risks because of the amount of information involved.

Likewise, the principle of accuracy also plays a primary role because the result of automated decision-making is strongly influenced by the quality of data. Data mining techniques rely on various sources such as social media and other third-party sources that are known for not always being accurate. The pluralism of data sources increases the risk of dealing with inaccurate data.[128] This problem does not only occur ex ante when collecting and analysing data but also ex post due to the distorted effects that inaccurate data can have on the outputs.[129] According to Tene and Polonetsky, 'in a big data world, what calls for scrutiny is often the accuracy of the raw data but rather the accuracy of the inferences drawn from the data'.[130]

[124] Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Wolter Kluwer 2002).
[125] Hildebrandt (n. 122).
[126] GDPR (n. 11), Art. 4(f).
[127] Ibid., Arts. 5(1)(e), 5(1)(f).
[128] Boyd and Crawford (n. 55).
[129] Ibid., 662.
[130] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 239.

All these principles should be read in light of the principle of the data controller's accountability, which is the ground upon which the GDPR's risk-based approach is built. The data controller should be able to prove compliance with general principles. The meaning of the principle of accountability can be better understood when focusing on the dynamic definition of the controller's responsibility based on the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[131]

On this basis, the data controller is required to implement appropriate technical and organisational measures to guarantee, and be able to demonstrate, that the processing is carried out in accordance with the GDPR and, especially, its principles. According to the principle of privacy by design and by default,[132] the data controller is required to set adequate technical and organisational measures, such as pseudonymisation, to implement the principles of data protection effectively and to provide the necessary guarantees by design and ensure that, by default, only the personal data necessary for each specific purpose are processed. For example, as far as the principles of transparency or purpose limitation are concerned, data processing should allow the data subject to be aware of the modality of processing even when artificial intelligence technologies are involved, thus requiring these technologies to take into consideration the requirement established by the GDPR. In other words, these principles would require data controllers to ensure ex ante that the implementation of technologies processing personal data complies with the general principles of European data protection law. However, there is a tension with general principles when data controllers rely on algorithmic technologies to process personal data.

These considerations could be enough to explain the clash between artificial intelligence and European data protection. Nevertheless, the implementation of algorithmic technologies for processing personal data is also relevant for the protection of data subjects' rights, precisely when these systems lead to significant legal effects on their rights and freedoms.

6.4.3 The Freedom from Algorithmic Processing

One of the primary constitutional challenges for privacy and data protection in the age of Big Data consists exactly of dealing with the lack of transparency and accountability in automated decision-making

[131] Ibid., Art. 24.
[132] GDPR (n. 11), Art. 25.

processes and their effects on individual fundamental rights and freedoms as well as democratic values. As already stressed, the involvement of algorithmic processing for purposes of profiling and automated decision-making challenges privacy and data protection.[133]

Automated decision-making could be defined as the process of making decisions without human intervention. According to the GDPR, this process consists of a decision based solely on automated processing.[134] Usually, these processes involve the use of artificial intelligence technologies. These techniques can lead to binding decisions also depriving individuals of legal rights such as accessing credit.[135] It is in this case that the GDPR aims to introduce safeguards to protect individuals against the discretionary use of personal data for purposes of automated decision-making. In order to empower data subjects to maintain control over their data and mitigate the asymmetry between the data controller and subject, the GDPR provides the so-called data subjects' rights.[136]

The GDPR is particularly concerned by profiling which consists of 'any form of automated processing of personal data consisting in the use of such personal data to evaluate certain personal aspects relating to a natural person, precisely, to analyse or foresee aspects concerning professional performance, the situation economic, personal health, preferences, interests, reliability, behaviour, location or movements'.[137] Against such processing, the data subject has the right to object at any time, for reasons connected with their particular situation. However, this right is not absolute since it can only be exercised when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,[138] or for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.[139] Therefore, the scope of such a right is narrow and does not apply when profiling occurs

[133] Bart W. Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27(1) Computer Law & Security Review 45.
[134] GDPR (n. 11), Art. 22.
[135] Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41 Science, Technology, & Human Values 118.
[136] GDPR (n. 11), Arts. 15–22.
[137] Ibid., Art. 4(4).
[138] Ibid., Art. 6(1)(e).
[139] Ibid., Art. 6(1)(f).

based on the consent of the data subject or any other legal basis provided for by the GDPR.

Once the right to object has been exercised, the data controller cannot process personal data unless it demonstrates the existence of legitimate reasons prevailing over the interests, rights and freedoms of the interested party or to ascertain, exercise or defend a right in court. Furthermore, if personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data for these purposes, including profiling. In both cases, the data controller is explicitly required to present this information clearly and separately from any other information at the time of the first communication with the data subject.

Such a right aims to empower users who can complain about the processing of their personal data when it is made by a public authority or it is the result of the choice of data controllers to rely on the legitimate interests as a legal basis of the processing, which, in any case, needs to balance the interest of the controller with the fundamental rights of the data subject. In this case, the right to object allows users to intervene in this balancing which, otherwise, would be left in the hands of data controllers. In this case, the right to object protects data subjects against profiling by artificial intelligence technologies, even if the scope of this right is narrow.

Together with this safeguard, under the GDPR, individuals can rely on their right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern him or her, or that significantly affects his or her person.[140] The WP29 has clarified that the reference to the expression 'right' not to be subject to a decision based exclusively on automated processing does not imply that this guarantee only applies when the subject invokes this right, since 'individuals are automatically protected from the potential effects this type of processing may have'.[141] As pointed out by Mendoza

[140] Stephan Dreyer and Wolfgang Schulz, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole' (2019) Bertelsmann Stiftung www.bertelsmann-stiftung.de/doi/10.11586/2018018 accessed 21 November 2021; Isak Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiani Synodinou and other (eds.), EU *Internet Law: Regulation and Enforcement* 77 (Springer 2017).

[141] Working Party Article 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2018), 20 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 accessed 21 November 2021.

and Bygrave, it is more appropriate to think of this safeguard as a prohibition rather than a right.[142] In this context, the principle of transparency would require the data controller to provide information to the data subject 'on the logic used, as well as the importance and the expected consequences of this treatment for the data subject', regardless of whether the data is collected by the data subject,[143] in line with the spirit of the GDPR which requires a high level of transparency in the processing of personal data.

By arguing *a contrario*, the lack of such a right would produce negative effects not only for individuals but also for democratic values since it would leave data controllers to fully rely on artificial intelligence technologies to make decisions affecting the rights of data subjects without providing any safeguards such as transparency and accountability for these outcomes. The lack of these safeguards is particularly evident when looking, for instance, at the framework of content moderation as examined in Chapter 5. This freedom can be considered as the positive translation of constitutional rights within the legal regimes of data protection and, therefore, it applies to private actors without the need to rely on the horizontal application of fundamental rights. In this sense, the right not to be subject solely to automated decision-making processes increases the possibility for data subjects to receive information about the automated decisions involving them and, therefore, fosters the level of transparency and accountability.

Therefore, even if the relevance of this right within the framework of the GDPR is clear, the remaining question concerns the degree of transparency which the data controller should ensure. According to the GDPR, the data controller should provide meaningful information about the logics involved in the decision-making process.[144] In order to ensure transparency and fairness, these logics should take into account the circumstances and context of the processing, implementing appropriate mathematical or statistical procedures for the profiling, technical and organisational measures appropriate to minimise errors and inaccuracies, as well as safe procedures for personal data to prevent, inter alia, discriminatory effects.[145]

The right not to be subject solely to automated decision-making has triggered a debate on whether the GDPR provides an effective legal basis

[142] Mendoza and Bygrave (n. 140).
[143] GDPR (n. 11), Art. 13(2)(f), Art. 14(2)(g), Art. 15(1)(h).
[144] Ibid., Recital 71.
[145] Ibid.

for data subjects to avoid potentially harmful consequences deriving from the implementation of algorithms, most notably by relying on a 'right to explanation' in respect of automated decision-making processes.[146] Some argue that the GDPR introduces it.[147] Others underline that such a right fosters qualified transparency over algorithmic decision-making,[148] deny the existence of such a right,[149] or doubt that the GDPR provisions provide a concrete remedy to algorithmic decision-making processes.[150]

It is not by chance that transparency is one of the most debated issues when focusing on algorithmic technologies.[151] The threats to individuals are intimately, even if not exclusively, connected with the impossibility to ensure transparent outcomes of automated decision-making processes.[152] Despite the criticisms of the process of mandatory disclosure,[153] these obligations constitute a first step to mitigate the asymmetries between data subjects and data controllers. The GDPR aims to empower data subjects by mitigating the technical opacity of automated decision-making.[154] The data controller should not only disclose the data used and the purposes of the processing, but it has

[146] See Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-making and a "Right to Explanation"' (2016) 38(3) AI Magazine 50.

[147] Mendoza and Bygrave (n. 140); Andrew D. Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143.

[148] Margot E. Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkley Technology Law Journal 189.

[149] Sandra Wachter and others, '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.

[150] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.

[151] See, e.g., Daniel Neyland, 'Bearing Accountable Witness to the Ethical Algorithmic System' (2016) 41 Science, Technology & Human Values 50; Mariarosaria Taddeo, 'Modelling Trust in Artificial Agents, a First Step Toward the Analysis of E-Trust' (2010) 20 Minds and Machines 243.

[152] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society https://journals.sagepub.com/doi/full/10.1177/2053951715622512 accessed 21 November 2021; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus and others (eds.), *Digital Enlightenment Yearbook* (IOS Press 2012).

[153] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250.

[154] Edwards and Veale (n. 150).

also the duty to inform the data subjects about the use of automated decision-making and explain the logic of this process. These safeguards constitute a shield against potential predetermined and discretionary decisions against which the data subject would not have any remedy.

A further guarantee for data subjects against automated decision-making is provided by the limitation to the processing of particular categories of data provided for by the GDPR, without prejudice to the cases of explicit consent of the data subject and if the processing is necessary for reasons of significant public interest on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject.[155] In the field of Big Data analytics, profiling aims to create clusters of individuals based on their characteristics. Often, processing telephone numbers or names and surnames would not be enough to develop predictive models since profiling focuses on the individual characteristics which constitute particular categories of data such as health information, political ideas or even biometric data. Even in these cases, adequate measures have to be in force to protect the rights, freedoms and legitimate interests of the data subject.

Nevertheless, this data subjects' right is not absolute. The general notion of 'legal or similarly significant effects' limits its general applicability.[156] The WP29 has also specified that this freedom applies just in cases of 'serious impactful effects' and when the automated decision could 'significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals'.[157] For example, this provision would apply when the data subject is applying for a credit card as well as accessing to education or health services.

Moreover, several exceptions limit the scope of data protection safeguards. Unlike the case of the notion of personal data and general principles, the GDPR provides a clearer set of exceptions to the application of this data subjects' right against automated decision-making processes. This liberty does not apply when the automated decision is

[155] GDPR (n. 11), Arts. 9(2)(a), 9(2)(g).
[156] Ibid.
[157] Ibid.

necessary for the conclusion or execution of a contract between the interested party and a data controller as well as when it is authorised by Union or Member State law to which the data controller is subject, which also specifies appropriate measures to protect the rights, freedoms and legitimate interests of the data subject. Moreover, this safeguard also does not apply when the processing is based on the explicit consent of the data subject. However, when the processing is based on a contract or the explicit consent of the data subject, the data controller is required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In this case, this prohibition turns into a right when the GDPR recognises that the data subject should at least have the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. This data subject's safeguard cannot lead to 'fabricating human involvement' since human involvement and oversight should be meaningful.

Furthermore, the data controller may limit the boundary of the right to explanation by invoking its interest to protect the trade secrets and intellectual property rights,[158] or, more generally, its freedom of economic initiative that would be frustrated by complying with transparency obligations requiring unreasonable resources.[159] For instance, when the techniques of data analysis through machine learning are involved, it is possible to highlight the so-called black box effect consisting of the impossibility to reconstruct the steps from the beginning of the processing up to the final output.[160] Bathaee underlined that this issue 'poses an immediate threat to intent and causation tests that appear in virtually every field of law'.[161]

This scenario is made even more opaque and fragmented by the limits that Member States establish to these data subjects' rights.[162] Member States can restrict such rights to the extent that limitations are established by EU law or the Member State, provided that this restriction respects the essence of fundamental rights and freedoms and a necessary and proportionate measure in a democratic society to

[158] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).
[159] GDPR (n. 11), Recital 63.
[160] Pasquale (n. 107).
[161] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology 890.
[162] GDPR (n. 11), Art. 23.

safeguard interests such as, for example, national security.[163] Therefore, on the one hand, the rights to data subjects against automated processing can mitigate the interferences coming from processing of personal data through algorithmic technologies. On the other hand, the scope of these rights could undermine the concrete enforcement of this safeguard, thus increasing the possibility for data controllers to rely on automated decision-making technologies to process personal data. Besides, the lack of legal certainty around the scope of this safeguard could also affect the consistent application of this safeguard as also demonstrated by the complexity of multi-state profiling.[164]

Within this framework, the challenges raised by automated decision-making processes are another example of the clash between algorithmic technologies and the protection of fundamental rights and democratic values. This case is another example of how European digital constitutionalism is called to reframe the role of European data protection in the algorithmic society.

6.5 The Constitutional Reframing of the GDPR

The analysis of the constitutional challenges of algorithmic technologies has underlined the limits of European data protection law in relation to the exercise of powers in the field of data. A stand-alone reading of the GDPR can only provide a partial view which could not solve the tension with the principle of the rule of law. The constitutional dimension of Big Data leads to examining the role of European digital constitutionalism in providing an interpretative angle reframing the GDPR in the algorithmic society.

As examined in Chapter 2, in the field of data, the constitutionalisation of the Union has played a critical role in shifting the attention from an economic perspective to a fundamental rights system. Moving from the field of the law in the books to that of the law in action, the ECJ played a fundamental role in consolidating the right to data protection. From the first recognition of data protection as a fundamental right in

[163] Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35(5) Computer Law & Security Review 105327.

[164] Reuben Binns and Michael Veale, 'Is that Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR' (2021) International Data Privacy Law https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipab020/6403925?login=true accessed 21 November 2021.

the *Promusicae* case,[165] even without emancipating this right from the safeguard of private life,[166] the ECJ reinforced its protection as it appears particularly clear in the decisions on digital privacy which followed the entry into force of the Lisbon Treaty.[167] The constitutional path of the protection of personal data reached a further step not only in the aftermath of Lisbon, but also with the adoption of the GDPR whose first aim is to ensure the right to protection of personal data as data subjects' fundamental rights.[168]

The codification of a new approach in the GDPR is not enough to assess the degree of protection in the European context but needs to be framed within the European constitutional matrix. Both judicial emancipation and legislative consolidation have led the protection of the fundamental rights to privacy and data protection to be a global model on which the European fortress of personal data is based as examined in Chapter 7. This is why the mere analysis of the GDPR can just provide a short answer about the role of European data protection. Here, European digital constitutionalism can provide the normative lens guiding European data protection which, despite its positive dimension, still needs to be constitutionally framed to face the asymmetry of power in the field of data.

The GDPR can be considered as the expression of a new societal *pactum*. It is no more enough to look at such fundamental rights in a negative vertical perspective, thus binding only public actors to individuals, but it is also necessary to look at them as triggers of a positive responsibility to intervene at the horizontal level to remedy the asymmetry of power fostered by the algorithmic society. In other words, by translating constitutional values in legal principles and rights, the GDPR is an expression of the new phase of European digital constitutionalism. The GDPR breaks the vertical nature of fundamental rights, recognising that individuals need to be protected by automated

[165] C-275/06 *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU* (2008) ECR I-271. Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds.), *Reinventing Data Protection* 3 (Springer 2009).

[166] *Promusicae*, ibid. According to para. 63: 'However, the situation in respect of which the national court puts that question involves, in addition to those two rights, a further fundamental right, namely the right that guarantees protection of personal data and hence of private life'.

[167] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart 2021).

[168] GDPR (n. 11), Recitals 1–2.

decision-making not only when performed by public actors but also when performed by powerful private companies such as online platforms.

When applying these considerations to data protection law, it is necessary to look at the European constitutional framework, precisely the constitutional values underpinning the GDPR. The primary purpose of data protection law is to protect autonomy while ensuring transparency and accountability. As a result, the following subsections provide a teleological interpretation of the GDPR under the lens of European digital constitutionalism. This approach would shed light on the constitutional values underpinning the GDPR and on how they can contribute to providing a constitutional-oriented interpretation mitigating the exercise of powers in the algorithmic society.

6.5.1 Recentring Human Dignity

The evolution of the algorithmic society has contributed to underlining the relevance of data as a personal piece of information. Increasingly, public and private actors rely on machines to make decisions on individual rights and freedoms based on the processing of data. While public actors trust algorithmic technologies to improve public services and perform public tasks such as biometric surveillance, private actors implement automated decision-making to process data to attract revenues following the logic of digital capitalism.[169] Within this framework, as underlined by Gutwirth and De Hert, 'humans have become detectable, (re)traceable and correlatable'.[170] Personal data disseminated in daily lives are raw materials for artificial intelligence systems which then are trained to cluster this data based on correlation. Nonetheless, since, in the age of Big Data, even generic pieces of information could be considered personal, clustering data also mean profiling individuals.

In Europe, personal data are 'personal' since they are connected to the individual. This focus is not only because the notion of personal data extends far beyond the notion of identified natural persons but also because data protection law without personal data would lose its constitutional meaning within the European framework. It is not by chance

[169] Jathan Sadowski, 'When Data Is Capital: Datafication, Accumulation, and Extraction' (2019) 6 Big Data & Society 1.
[170] Gutwirth and De Hert (n. 106), 287.

that the scope of the GDPR does not extend to legal persons or deceased,[171] or non-personal data.[172] This characteristic underlines how, in Europe, personal data are not only relevant for the circulation of information or the extraction of value. As stressed in Chapter 3, the rise of European digital constitutionalism has shed light on the constitutional dimension of privacy and data protection complementing the internal market goals.

This constitutional framework is the reason why personal data cannot be seen just as an object of property rights but also as data 'extra commercium'.[173] The 'propertisation' of personal data contributes to their commodification under the logic of digital capitalism with the result that any data would be considered as tradable as goods and not as a piece of individual identity. It is true that the circulation and exchange of personal data constitute the pillars of the algorithmic society. Nonetheless, the unaccountable and discretionary commodification of personal data would lead to considering consumer protection or contract law as the primary instrument to deal with the commercial exploitation of data.[174] However, these concurring regimes would fail to protect personal data as an expression of the individual and, therefore, this is also why personal data 'cannot be considered as a commodity'.[175] Likewise, the EDPS has underlined that personal data cannot be conceived as mere economic assets.[176] As Floridi underlined, '"My" in my data is not the same as "my" in my car, but it is the same as

[171] Bart van der Sloot, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System' (2015) 31 Computer Law and Security Review 26.

[172] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303/59.

[173] Václav Janeček and Gianclaudio Malgieri, 'Data Extra Commercium' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), *Data as Counter-Performance – Contract Law 2.0?* 93 (Hart 2020).

[174] Yves Poullet, 'Data Protection Between Property and Liberties. A Civil Law Approach' in Henrik W. K. Kaspersen and Anja Oskamp (eds.), *Amongst Friends in Computers and Law. A Collection of Essays in Remembrance of Guy Vandenberghe* 160 (Kluwer Law International 1990); Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011).

[175] 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 (2019) OJ L 136/1, Recital 24.

[176] European Data Protection Supervisor, 'Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (23 September 2016) https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf accessed 21 November 2021.

"my" in my hand'.[177] Therefore, protecting the right to privacy should be considered as a matter of personal identity and integrity since it determines the evolution of human personality and therefore of human dignity. In a different way, the right to be forgotten exactly showed this face of the right to privacy even before the rise of online platforms, and the *Google Spain* case.[178]

Even if human dignity is almost invisible in the GDPR,[179] the human-centric approach in European data protection law comes from the ability of human dignity to permeate in the core of European fundamental rights.[180] The Charter opens up the catalogue of rights stating 'human dignity is inviolable. It must be respected and protected'.[181] The central position of this value within the Charter is not a formal recognition of constitutionality,[182] but it plays the role of a pillar for the entire system of fundamental rights. This approach mirrors the Universal Declaration of Human Rights which enshrines human dignity in its preamble.[183] Therefore, as stressed in Chapter 1, human dignity should not be seen as a clashing value but as the core of each fundamental right laid down in the Charter. Human dignity therefore is a necessary piece of the puzzle to be considered and safeguarded in the balancing process. This is part of the European constitutional roots which look at dignity as the pillar against any human annihilation.

Therefore, the mission of data protection law would be to ensure that its human imprinting does not fall apart while ensuring democratic values of transparency and accountability. Even in this case, the role of dignity could be considered as a primary trigger for the consolidation of data protection as the positive dimension of the right to privacy,

[177] Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy of Technology 307, 308.

[178] Franz Werro, 'The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash' in Aurelia Colombi Ciacchi and others (eds.), *Liability in the Third Millennium, Liber Amicorum Gert Bruggemeier* 285 (Nomos 2009).

[179] GDPR (n. 11), Art. 88. This provision requires Member States to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context 'to safeguard the data subject's human dignity, legitimate interests and fundamental rights'.

[180] Stefano Rodotà, *Vivere la democrazia* (Laterza 2019); Catherine Dupré, *The Age of Dignity Human Rights and Constitutionalism in Europe* (Hart 2015).

[181] Charter (n. 36), Art. 1.

[182] Case C-377/98 *Netherlands* v. *European Parliament and Council* (2001) ECR I-7079, 70–77.

[183] Universal Declaration of Human Rights (1948): 'Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world'.

similarly to how human dignity could contribute to fostering the positive dimension of the right to freedom of expression to address the challenges of content moderation as examined in Chapter 5. According to the EDPS, '[p]rivacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing'.[184]

The notion of personal data is not the only point showing the role of human dignity in the GDPR. Individual consent is the primary pillar of European data protection law, thus representing the centrality of individual self-determination.[185] As mentioned in Chapter 1, the first decision of the German Constitutional Court on data protection has shed the light on the role of dignity in the processing of personal data. It is indeed the autonomous choice of the data subject which would allow the data controller to legally process personal data. This is why, even if imbalances of power question the meaning of consent in European data protection law, the GDPR still focus on consent as a primary legal basis defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[186]

Likewise, the distinction between personal data and particular categories of data provides another clue about the human-centric approach of European data protection law. This double track of protection for personal data aims to protect personal information which can reveal intimate aspects of human lives. Such a difference, already introduced in the Data Protection Directive, has been fostered by the GDPR which has not only extended the categories of data falling under the scope of such a special regime but also provides a general ban of the processing of this type of data even though it foresees conditions of lawfulness as exceptions.[187] For instance, biometrics and DNA data have been included within the broader protection of particular categories of data, being it information able to represent humans as they are.

[184] European Data Protection Supervisor, 'Opinion 4/2015. Towards a new Digital Ethics' (11 September 2015) https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf accessed 21 November 2021.
[185] Yves Poullet, 'Data Protection Legislation: What is at Stake for our Society and Democracy' (2009) 25 Computer Law & Security Review 211.
[186] GDPR (n. 11), Art. 4(11).
[187] Ibid., Art. 9.

Precisely, in a phase where biometric technologies are expanding and intertwining with artificial intelligence to pursue different tasks,[188] such a safeguard reflects the need to avoid that personal data are subject to automated decisions without the 'explicit consent' of data subjects. In this case, it is not enough to rely on the conditions for processing personal data, but it is necessary to ground the processing on specific legal bases.[189] Even in this case, the core of the entire system is the data subject's consent, which, in this case, has to be 'explicit'.

Such a personalistic approach also affects the framework of automated decision-making processing. The GDPR does not expressly clarify the constitutional values underpinning its structure. Therefore, a literal or systemic interpretation of data protection law could not provide a full picture of the values which the prohibition to subject individuals to these systems would protect. Dreyer and Schulz have underlined that the goal of this rule is beyond the mere protection of personal data.[190] Even if not exclusively, the primary goal of this rule is the protection of human dignity. The right not to be subject to automated decision-making deals with the ability of machines to make determinations about human lives. Even in this case, the rise of the Internet has underlined how digital technologies can perform activities in a more efficient way than humans. The same is true for algorithmic technologies that are able to see correlations that humans do not perceive, or predict the future which is one of the abilities that humans have always tried to reach.

What does not actually change is the risk of error. Even if machines were more efficient than humans, they could still fail and reproduce the biases of their programmers. At first glance, algorithms would appear as neutral technologies which can extract values from information that are useful for businesses and society. However, from a technical perspective, algorithms are far from being neutral. They are not just mathematical models providing outcomes in a certain form based on the processing of information.[191] Algorithms transform inputs into outputs, thus expressing a value judgement. Automated decision-making

[188] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis* (Springer 2013).
[189] GDPR (n. 11), Art. 9(2).
[190] Dreyer and Schulz (n. 140).
[191] Tarleton Gillespie, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J. Boczkowski and Kristen A. Foot (eds.), *Media Technologies: Essays on Communication, Materiality, and Society* 167 (MIT Press 2014).

systems are therefore value-laden.[192] The human role in the programming and development of these technologies contributes to reflecting the biases and values of programmers into the technological design.[193] This issue is not a novelty since all technologies are the result of certain design choices. Reidenberg and Lessig have already clarified how much the architecture of technology is a critical piece of the regulatory jigsaw.[194] In the case of algorithms, the role of design is even more critical since these technologies can produce decisions on which humans ground their activities, or even largely rely.[195]

Besides, machines are still not entirely able to interpret real dynamics and exactly understand contexts and emotions,[196] or translating legal concept into machine determinations.[197] This limit also explains why so frequently the implementation of artificial intelligence technologies has led to discrimination.[198] The right to equality can be considered another expression of human dignity. Without being considered equal, there are multiple layers of protection for different categories of 'humans'. The right to non-discrimination is one of the fundamental principles of European constitutional law. The right to equality is the basic pillar of democratic constitutionalism as shown by its relevance in the Charter and the Convention.[199] Discriminatory outcomes of

[192] Brent D. Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679 accessed 22 November 2021.

[193] Pasquale (n. 107).

[194] Lawrence Lessig, *Code: And Other Laws of Cyberspace. Version 2.0* (Basic Books 2006); Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997–8) 76 Texas Law Review 553.

[195] John Zerilli and others, 'Algorithmic Decision-Making and the Control Problem' (2019) 29 Minds and Machines 555.

[196] Andrew McStay and Lachlan Urquhart, 'This Time with Feeling? Assessing EU Data Governance Implications for Out of Home Emotional AI' (2019) 24(10) First Monday https://firstmonday.org/ojs/index.php/fm/article/download/9457/8146 accessed 21 November 2021.

[197] Simon Deakin and Christopher Markou, 'Ex Machina Lex: Exploring the Limits of Legal Computability' in Simon Deakin and Christopher Markou (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing 2020).

[198] Sandra Wachter, Brent Mittelstadt, Chris Russell, 'Why Fairness cannot be Automated: Bridging the Gap between EU Non-discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567; Andrea Romei and Salvatore Ruggieri, 'A Multidisciplinary Survey on Discrimination Analysis' (2014) 29 The Knowledge Engineering Review 582; Bart Custers and others (eds.), *Discrimination and Privacy in the Information Society* (Springer 2013); Kevin Macnish, 'Unblinking Eyes: The Ethics of Automating Surveillance' (2012) 14 Ethics and Information Technology 151.

[199] Charter (n. 36), Art. 20; Convention (n. 31), Art. 14.

algorithmic processing can originate from the low level of data quality or embedded bias in the programming phase like in the case of discrimination based on ethnicity.[200]

Therefore, the GDPR shields data subjects against the interference to their legal rights coming from the errors automated decision-making can produce. This prohibition recognises that machines cannot be fully trusted. In other words, such a rule clarifies that efficiency cannot prevail over fundamental rights and freedoms. At the same time, artificial intelligence technologies can also foster fundamental rights, thus allowing humans to escape from paths of marginalisation. Even in this case, the GDPR has not introduced a general ban for this type of processing but has tried to limit the serious effects that these technologies can produce on data subjects. Likewise, the GDPR has introduced the so-called human-in-the-loop principle to ensure that human decisions are not affected by decisions taken just by unaccountable systems. This approach is firmly connected with the acknowledgement that machines err and are (still) not able to distinguish the complexity of human lives. The attempts to digitise human lives to a mere calculation would annihilate the role of humans, leading towards a process of dehumanisation. In other words, the human being is *dignus*. Any attempt to digitise humanity would clash with the nature of human beings.

Within this framework, human dignity constitutes the primary beacon for data controllers and courts when focusing on the challenges of automated decision-making. This focus does not mean that this right should confer privacy and data protection a quasi-absolute protection in any case. On the opposite, privacy and data protection would acquire a predominant role when there is the need to ensure that individual rights are not so compressed that autonomy and self-determination are effectively compromised. The limit established by the GDPR to the processing of personal data through automated decision-making processes is not a mere data subject right which can be overcome easily by ensuring security measures or opaque forms of explanation. It is an instrument of freedom against the techno-determinism established by predominant private and public actors.[201] This rule horizontally connects human dignity, as the

[200] Raphaële Xenidis and Linda Senden, 'EU Non-discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination' in Ulf Bernitz and others (eds.), *General Principles of EU law and the EU Digital Order* 151 (Kluwer Law International 2020).

[201] Antoniette Rouvroy, 'Technology, Virtuality and Utopia: Governmentality in an Age of Autonomic Computing' in Mireille Hildebrandt and Antoniette Rouvroy, *Law, Human*

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

basic pillar of European constitutionalism, with algorithmic technologies, thus making the promises of a more constitutional sustainable innovation. The focus on human dignity would be the primary reference for lawmakers and judges in approaching this safeguard, thus implying a strict interpretation of the exceptions and limitations to this 'human' right.

6.5.2 Conflicting Positions and Proportionality

Human dignity is the primary but not the only underpinning value of the GDPR. Another constitutional principle grounding European data protection is proportionality which can be considered the foundation of the risk-based approach based on the principle of accountability. As in the case of human dignity, different angles can show how this value is expressed by the GDPR.

Proportionality is a pillar of democratic constitutionalism.[202] Even if this principle is declined in different ways on a global scale,[203] proportionality expresses the need to internally limit the exercise of public and private powers, thus safeguarding individuals against excessive interferences.[204] The structure of European data protection is a paradigmatic example of the principle of proportionality. As already stressed, personal data enjoy a broad margin of protection in the Union.

Although the ECJ has recognised a high degree of protection to personal data, there is not a rigid hierarchy between fundamental rights and freedoms. Data protection is not an absolute right even when focusing on legitimate interests according to the tests established by the Convention and the Charter. The protection of this fundamental right cannot lead to the destruction of other constitutional interests such as freedom to conduct business as enshrined in the Charter.[205]

Therefore, when interpreting the obligations of the GDPR, it is crucial not to forget that the interests of the data controller and of the data

Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology (Routledge 2011).

[202] Stephen Gardbaum, 'Proportionality and Democratic Constitutionalism' in Grant Huscroft and others (eds.), *Proportionality and the Rule of Law. Rights, Justification, Reasoning* 259 (Cambridge University Press 2014).

[203] Alec Stone Sweet and Jud Mathews, *Proportionality Balancing and Constitutional Governance. A Comparative and Global Approach* (Oxford University Press 2019).

[204] Vicki C. Jackson and Mark Tushnet (eds.), *Proportionality: New Frontiers, New Challenges* (Cambridge University Press 2017); Aharon Barak, *Proportionality Constitutional Rights and their Limitations* (Cambridge University Press 2012); Robert Alexy, *A Theory of Rights* (Oxford University Press 1985).

[205] Charter (n. 37), Art. 16.

subject represent nothing but the constitutional clash between the protection of personal data with other fundamental rights and freedoms or legitimate interests in the case of public authorities. In other words, the general principles, safeguards and obligations of the GDPR need to be framed within such a context of balancing rather than axiology. It is not by chance that the ECJ has relied on the principle of proportionality since its first cases on data protection,[206] and this balancing logic is at the core of the GDPR's structure.

Moving from the constitutional level to the GDPR, the principle of accountability of the data controller could be considered the constitutional translation of a risk-based approach based on the notion of balancing. This principle requires the controller to prove compliance with the GDPR's principles by establishing safeguards and limitations based on the specific context of the processing, primarily the risks for data subjects.[207] The Data Protection Directive had already tried to introduce such an approach focused on the risk of processing, for instance, concerning the implementation of security measures. Likewise, the WP29 stressed the role of a risk-based approach in data protection underlining how risk management is not a new concept in data protection law.[208] Even the Council of Ministers of the Organisation for Economic Co-operation and Development implemented a risk-based approach when revising the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, first adopted in 1980.[209]

From a formal perspective, despite the open clauses, the move from minimum to full harmonisation has been a powerful boost for legal certainty in the internal market. Such a move has not only led to strengthening the protection of privacy and personal data as fundamental rights of the Union but has also allowed a more balanced approach between rights and obligations. The principle of accountability reflects such a mix between certainty and proportionality. The data controller

[206] Charlotte Bagger Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 International Data Privacy Law 239.

[207] Raphael Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

[208] Working Party Article 29, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (30 May 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf accessed 21 November 2021.

[209] OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed 21 November 2021.

has been considered responsible (and not only liable) to ensure that the protection of data subject's privacy and data protection are ensured and protected. And this role comes from the respect not only of the GDPR's obligations but also of general principles.

The GDPR modulates the obligations of the data controller according to the specific context in which the processing takes place, namely 'taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural person'.[210] For instance, when looking at legitimate interest as a condition for lawfully processing personal data, the GDPR provides a limitation balancing 'the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.[211] This focus extends also to the principle of privacy by design and by default as an expression of the general principle of accountability.[212] As observed by Macenaite, 'risk becomes a new boundary in the data protection field when deciding whether easily to allow personal data processing or to impose additional legal and procedural safeguards in order to shield the relevant data subjects from possible harm'.[213] It would be enough to focus on the norms concerning the Data Protection Impact Assessment or the appointment of the Data Protection Officer to understand how the GDPR has not introduced mere obligations to comply but a flexible risk-based approach which leads to defining different margins of responsibility on each data controller depending on the context at stake.[214]

[210] GDPR (n. 11), Art. 24(1).

[211] Ibid., Art. 6(1)(f).

[212] Ibid., Art. 25. Ira S. Rubinstein, 'Regulating Privacy by Design' (2012) 26 Berkeley Technology Law Journal 1409; Ugo Pagallo, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds.), *European Data Protection: In Good Health?* 331 (Springer 2012).

[213] Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8(3) European Journal of Risk Regulation 506.

[214] Working Party Article 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (4 October 2017) http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 accessed 21 November 2021. See Ruben Binns, 'Data Protection Impact Assessment: A Meta-Regulatory Approach' (2017) 7(1) International Data Privacy Law 22; Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* 33 (Springer 2012).

Fundamental rights are the parameters on which the risk-based approach, as a system where data controllers' responsibility is assessed on a case-by-case basis, is grounded. This system represents nothing but the expression of a principle of proportionality reflecting the lack of a rigid axiology in the European constitutional framework. The risk-based approach reflects nothing else than the balancing of the conflicting interests of data subjects and controllers. In other words, the GDPR has led to the merge of a rights-based approach where the fundamental rights of data subjects play the role of a beacon for compliance.

From the perspective of data controllers, the high standard of compliance required by the GDPR could however affect small or medium controllers which can be required to adopt higher safeguards, primarily when data processing operations could lead to high risks for the data subjects. This approach could affect the freedom to conduct business and development of the internal market. Even if the GDPR's approach could favour multinational corporations in the process of compliance,[215] nevertheless, it introduces a mechanism which does not focus only on rigid obligations but also on the concrete framework of the processing. This margin of discretion could promote the development of artificial intelligence technologies while protecting individual fundamental rights. This shift from theory to practice introduces certain flexibility allowing the data controller to determine the measures to apply according to the risks connected to data processing, while maintaining the duty to justify the reasons for these decisions. The GDPR would increase the discretion of the data controller in determining which safeguards apply to the data collected and processed in a certain context.

Likewise, from the data subjects' standpoint, the risk-based system is complemented by a rights-based system coming from the broad extension of fundamental rights in the European framework. Individuals have the right to access and limit the processing of their data, ask about their erasure or portability based on the conditions established by the GDPR for each data subject's right. Scholars have underlined that 'from the user perspective, the impact of data portability is evident both in terms of control of personal data (and in general in the sense of empowerment of control rights of individuals), and in terms of a more user-centric interrelation between services. At the same time, it is

[215] Michal S. Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349.

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

a challenge to third data subjects' rights'.[216] This approach underlines how the GDPR does not provide users with absolute rights. While empowering data subjects would increase the control over the processing of data, the implementation of their rights is a burden requiring data controllers to invest resources and define procedures to implement them.

When framing such considerations in the field of artificial intelligence, the GDPR does not establish an absolute prohibition in relation to automated decision-making, even if it bans the processing of particular categories of data except for the case where the data subject has given his or her explicit consent. The GDPR introduces exceptions according to which, despite potential legal or similarly significant consequences, data subjects cannot rely on this right. Their presence should not come as a surprise when focusing on the characteristics of European constitutionalism which, as already stressed, does not recognise absolute protection to fundamental rights. The ECJ underlined that the right to the protection of personal data does not enjoy absolute protection but is subject to balancing with other interests.[217] In any case, limitations shall be strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality.[218] Moreover, Member States can introduce exceptions to limit the right not to be subject to automated decision-making processes.[219] In any case, the protection of fundamental rights cannot lead to the annihilation of any other rights and freedoms recognised in this Charter.

Therefore, the principle of accountability is not only a burden for data controllers but also a threatening delegation of responsibility concerning the protection of fundamental rights and freedoms. This way, the GDPR leads data controllers to become the arbiters of privacy and data protection. The limit to the exercise of this power is the principle of proportionality which, together with human dignity, are guidance for lawmakers and judges when addressing the balancing between the accountability of data controllers and the fundamental rights of data subjects. Therefore, the principle of accountability can play an important role in the development of the internal market without leaving

[216] Paul De Hert and others, 'The Right to Data Portability in GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34(2) Computer Law & Security Review 193, 197.

[217] Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* (2010) ECR I-11063. See GDPR (n. 11), Recital 4.

[218] Charter (n. 36), Art. 52.

[219] GDPR (n. 11), Art. 23.

fundamental rights behind. As a general principle, the more the discretion exercised by the data controller, the more the data subjects should be protected. This principle would leave data controllers to perform their activities considering that their beacon of compliance is not simply represented by the GDPR's material and organisational requirements but also coincides with the protection of individuals, precisely their dignity.

Therefore, the principle of human dignity is relevant within the framework of proportionality. Although the GDPR's exceptions to data subjects' rights and freedoms may find their legitimation in the need to balance conflicting interests, however, justifying exceptions to data subjects' rights against automated decision-making processes would betray the aim to protect human dignity. It would be worth wondering how exceptions could be tolerated in this case if these technologies could lead to a process of dehumanisation in the long run. The answer to such a concern can be found by looking at due process safeguards which would aim to preserve human dignity while promoting a sustainable solution to foster innovation.

6.5.3 Enhancing Due Process

The question is therefore how human dignity can be protected against potential disbalances in the exercise of conflicting rights and freedoms. Limitations to individual rights reflecting the principle of proportionality should not be considered as a threat to human dignity when due process safeguards are in place. The possibility to rely on procedural safeguards would mitigate disproportionate effects resulting from the exercise of public powers or private determinations. Due process would play a crucial role even beyond the boundaries of public powers.[220]

Together with the personalistic principle, European data protection law is an example of due process safeguards. Since the adoption of the Data Protection Directive, European data protection law has primarily provided substantive obligations and procedural safeguards regulating the entire process of data processing from analysis of risks (e.g. DPIA), to rules on notice (e.g. mandatory disclosure), collection (e.g. consent), processing (e.g. purpose limitation), safeguards (e.g. data subject rights) and remedies (e.g. judicial enforcement). These norms represent the expression of the right to self-determination of individuals who,

[220] Giacinto Della Cananea, *Due Process of Law Beyond the State: Requirements of Administrative Procedure* (Oxford University Press 2016).

without knowing how data are processed, cannot be aware of the processing of their personal data. These ex ante safeguards increase transparency and accountability, thus making the individual more aware of how personal data are used to make even automated decisions which could affect their legal rights. Put another way, such an approach would meet that principle of self-determination which makes humans *dignus* rather than subject to public and private determinations.

By promoting transparency and accountability in automated decision-making processes through procedural safeguards, the GDPR fosters human dignity. Therefore, due process is an essential tile of the constitutional mosaic of the GDPR. This constitutional architecture is also evident when focusing on the safeguards relating to artificial intelligence technologies. The data controller is required to inform data subjects about the existence of a process of automated decision-making, its logic, significance and consequences,[221] while the data subject has the right to ask the data controller to access their personal data.[222] In the case of the right not to be subject to automated decision-making, the GDPR recognises a procedural safeguard consisting of the right 'to require human intervention, to express her point of view and to contest the decision'.[223] Therefore, apart from when the processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, individuals have the right to ask for human intervention to assess the machine's outcome.[224]

The principle of human-in-the-loop in the context of algorithmic decision-making is a paradigmatic attempt to introduce procedural safeguards. Minimal due process becomes a precondition to mitigate the asymmetry of powers between individuals and data controllers in the context of automated decision-making.[225] In this sense, due process

[221] GDPR (n. 11), Art. 13.
[222] Ibid., Art. 15.
[223] GDPR (n. 11), Art. 22(3). See Ben Wagner, 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11(1) Policy & Internet 104; Fabio M. Zanzotto, 'Viewpoint: Human-in-the-loop Artificial Intelligence' (2019) 64 Journal of Artificial Intelligence Research 243.
[224] Meg L. Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216.
[225] Danielle K. Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington University Law Review 1; Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 Boston College Law Review 93; Danielle K. Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.

is an inalienable right in the algorithmic society,[226] or why individuals should have a right to contest artificial intelligence systems.[227] This constitutional value raised within the realm of state actor is horizontally extended to the private actors through the obligation to ensure human intervention. It is not by chance that this principle is stated only when the processing involved automated decision-making technologies. This is because algorithmic decisions can produce serious effects on individual rights and freedoms. To remedy the lack of transparency oversight on algorithmic technologies, the GDPR requires that this processing deserves to be complemented by an adversarial principle and redress mechanism based on human intervention.

By recognising this right, the GDPR also seems to suggest that the last word over individual rights and freedoms should be human. A machine should not play this function without the support of humans that need to be in the loop. This is what the Commission already underlined in 1992 when stating that 'human judgment must have its place'.[228] Therefore, due process safeguards can protect human dignity complementing the general prohibition of full automated decision-making systems for the processing of personal data. This principle does not just recognise the role of humans in automated decision-making but also the primacy of human assessment over the efficiency of machines. Paradoxically, the inefficiency and irrationality of human beings is the last safeguard against the true interpretation of its nature.

The principle of human-in-the-loop cannot be considered as a general solution for the challenges raised by artificial intelligence. By looking at such a principle under the lens of proportionality, it can be observed that, while enhancing due process safeguards, it could potentially disregard other interests requiring protection. A broad extension of this rule can undermine the freedom to conduct business of private actors or the performance of public tasks. Besides, as already stressed, relying on human intervention as a procedural safeguard does not always ensure better decision-making.

[226] Frank Pasquale, 'Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication' in Hans-W Micklitz and others (eds.), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[227] Margot E. Kaminski and Jennifer M. Urban, 'The Right to Contest AI' (2021) 121(7) Columbia Law Review 1957.

[228] Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data COM(92)422 final, 26–7.

These drawbacks are just a small price to pay to ensure that humans are not marginalised by opaque algorithmic technologies and asymmetries of powers. These concerns are compensated by the critical role which due process plays against the unaccountable development of artificial intelligence technologies and the rise of private powers in the algorithmic society. The development of automated systems is not always driven by public purposes but usually by business interests focused on profit maximisation. Design choices could be not neutral and answer to opaque business logics which transform human life in technical norms of processing and extraction of values. In other words, the definition of transnational standards of automated systems outside any public scrutiny contributes to creating a para-constitutional environment competing with public values. This situation is not only relevant for due process, but also for the principle of the rule of law. If legal norms are replaced by technological standards, there will be no space for democratic constitutionalism to ensure the protection of public values against the rise of unaccountable technologies expressing private powers. Within this framework, the principle of human-in-the-loop is a shield not only as a due process safeguard, but also to protect democratic values.

The GDPR is fostering the principle of rule of law when the processing of personal data involves automated decision-making. This way, the GDPR bans any discretionary use of automated decision-making to process personal data. The principle of the rule of law is of a critical value to reduce the gap between the public and private sector involved in processing personal data. In the lack of any legal obligations, private actors are not required to give reasons justifying their policies or actions. While public actors are required to comply with constitutional principles, the private sector is not bound by constitutional principles and norms without a positive translation as it occurred with the GDPR. In the algorithmic society, private companies have demonstrated their abilities to acquire dominant positions in the market of data by extracting value from them. Within this framework, the data subject could be considered as a vulnerable actor whose protection of rights and freedoms should not only find its ground in the substantive rights but also in procedural safeguards to remedy the imbalance of power.

Within this framework, enhancing due process complements the relevance of human dignity and proportionality as expression of the constitutional values underpinning the GDPR. In this case, the GDPR

obligations should not be seen as a mere instrument for requiring data controllers to comply with certain rules but as the constitutional expression of procedural safeguards aimed to avoid a disproportionate exercise of powers in the balancing between conflicting interests. In this sense, the obligations of the GDPR should be constitutionally interpreted as a means to ensure that human dignity and democratic values are not annihilated by the lack of transparency and accountability in the exercise of powers in the field of data.

6.6 Constitutional Values in the Algorithmic Society

The implementation of algorithmic technologies in the processing of personal data has increased the concerns for individuals, who are subject to ubiquitous forms of control and surveillance, and democratic values. The role of algorithmic technologies for the fourth industrial revolution is not only relevant for the potentialities of these technologies but, as for the Internet at the end of the last century, also for its dissemination in society and commodification.[229] These technologies are no longer closed to the domain of academics or specific business sectors, but are spreading as expressions of powers thus reaching consumers, especially because of the need to gather data and information to train artificial intelligence technologies which can provide new models and predictive answers. One of the primary promises of these technologies is to help humans decide, for example, by replacing or solving complex questions through data analytics.[230]

Nonetheless, the massive implementation of these technologies does not always seem to bring positive effects, especially when looking at the protection of fundamental rights and democratic values. The challenges relating to the exercise of powers in the field of data challenges the right to privacy once again, thus requiring a positive approach to protect fundamental rights and democratic values. This is the result of the European process of constitutionalisation leading the protection of individual fundamental rights to be the beacon of data protection law. The rise and consolidation of European data protection has been a first

[229] Brandon Allgood, 'The Commoditization of AI and The Long-Term Value of Data' Forbes (10 April 2017) www.forbes.com/sites/forbestechcouncil/2017/04/10/the-commoditization-of-ai-and-the-long-term-value-of-data/#74c71abd159c accessed 21 November 2021.

[230] Brian Cantwell Smit, *The Promise of Artificial Intelligence. Reckoning and Judgment* (MIT Press 2019).

https://doi.org/10.1017/9781009071215.007 Published online by Cambridge University Press

answer to the challenges of automation. The constitutional evolution of data protection in the European framework shows the relevance of this fundamental right for safeguarding democratic values in a society which has strongly digitised in the last forty years. The ECJ has underlined a shift from the functional dimension of the Data Protection Directive, linked to the growth of the internal market, to a constitutional approach which has led to the adoption of the GDPR. Still, the modernisation of European data protection law fails to achieve the goal of protecting privacy and personal data in the lack of constitutional guidance.

The characteristics of European digital constitutionalism can provide an interpretative path to understand the role of data protection in the algorithmic society. The constitutional-oriented interpretation of the GDPR shows the horizontal underpinning values of the protection of privacy and data protection as fundamental rights, precisely human dignity, proportionality and due process. These values guiding European data protection can contribute to safeguarding the right of privacy and self-determination while breaking the asymmetries of powers threatening democratic values.

Therefore, the rise and consolidation of European data protection has not only led to an evolution of the constitutional paradigm but also to a translation of vertical constitutional values into horizontal principles and operational norms. This approach may protect the centrality of human dignity against the opaque and unaccountable processing of personal data in the hands of powerful actors, such as online platforms, while ensuring a proportionate approach to the conflicting rights at stake also thanks to due process safeguards.

Within this framework, the role of digital constitutionalism is far from being exhausted. Constitutional values have just started to imbue the algorithmic society and the European constitutional path is still at the beginning. A new phase of digital constitutionalism is likely around the corner.