UNIVERSITA' COMMERCIALE "LUIGI BOCCONI"

PhD SCHOOL

PhD program in Legal Studies

Cycle: 34°

Disciplinary Field (code): IUS/08

Individual control and data protection
Looking back and moving forward

Advisor: Prof. Oreste POLLICINO

PhD Thesis by

Maria Chiara MENEGHETTI

ID number: 3082959

Year 2022

A mio padre e mia madre

«Tous pour un, un pour tous»

Alexandre Dumas, “Les Trois Mousquetaires”, 1844

Acknowledgments

During my PhD journey, many people have crossed my path. All of them have left a mark, some of them deserve a special mention.

First, I would like to express my gratitude to my supervisor, Professor Pollicino, for his insights and guidance throughout this project.

A sincere thank you to Professor Bassini for the patience and time he was so kind to devote me during my research.

I would also like to show my appreciation to Professor Finocchiaro, who first introduced me to this field of law and pushed me to never settle.

I am extremely grateful to the amazing Phd friends and colleagues that Bocconi allowed me to meet and to share this challenging experience with. I will not forget you.

One of the most important thank you goes to my parents: you remain my unconditional backbone and main source of inspiration.

Last but not least thank to you, Mat. I could not have done this without you

Table of Contents

Table of abbreviations

General

AI	Artificial Intelligence
AIA	Algorithmic Impact Assessment
BEUC	*Bureau Européen des Unions de Consommateurs* - European Consumer Organisation
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ETiA	Ethical Impact Assessment
EU	European Union
HRIA	Human Rights Impact Assessment
IA	Impact Assessment
IoT	Internet of Things
NGO	Non-governmental organization
OECD	Organization for Economic Cooperation and Development
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
WP29	Article 29 Working Party

International law and EU law

1980 OECD Guidelines	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (original version of 1980)
AI Act	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)
Convention 108+	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2018)
DGA	Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)
DPD	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
DSA	Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC
DMA	Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)
e-Privacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
e-Privacy Regulation	Proposal for a Regulation of the European Parliament and

	of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
ECHR	European Charter of Human Rights
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	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)

Table of tables

INTRODUCTION

This work aims at investigating the concept of "individual control over personal data", as a core constituent of data protection law. We live in a time in which data have become a main driving force behind innovation, growth and prosperity. Companies and governments are at war to gain new usable knowledge. Technological advances are upstaging expectations in terms of what can be inferred, predicted and manipulated through data and people are milked at an increasing speed to fulfil the generalized data hunger. As a result, calls to bring individuals back in control of their personal data and to develop a more individual-friendly data ecosystem have been increasingly pressing. Yet, older and newer hurdles continue to interfere in the successful implementation of this vision.

Generally speaking, the notion of "control" is employed to refer to situations of "power over something or someone", consequently to the "ability to determine what others should do or how things should be done"[1]. Starting from this general construction, in the context of personal data[2] this notion can assume different – if not opposite – meanings.

A first way of considering the concept of control typically emphasizes its connection to the risks deriving from the emergence of the so-called "surveillance society"[3], namely a society characterized by mass collection, recording and analysis of information to monitor and govern individuals. In these terms, *control* becomes a synonym of *surveillance* and *social control.* It identifies the power of public institutions and private companies to surveil, regulate, manage and influence people's behaviour through the use of their personal data. Fears for the rise of a *surveillance state*, triggered by the first national initiatives of population census carried out around the '70s, were among the catalysts that led to the adoption of the first acts regulating the automated processing of personal data in Europe. Since then, practices of mass surveillance have grown in magnitude and intrusiveness. The 2013 Snowden's revelations on US National Security Agency (NSA) surveillance programmes confirmed this underground trend, prompting a much-needed discussion on the rightful balancing between security and privacy in a

---

[1] *Oxford English Dictionary*, 2nd ed. Oxford: Oxford University Press, 2004, s.v. "control".

[2] The term "personal data" refers to «any information relating to an identified or identifiable natural person», Art. 4(1), GDPR.

[3] David H Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (University of North Carolina Press 1989).

modern democratic state[4]. Next to the powers of public authorities, the exponential growth of private corporations in technological and economic power has given rise to advanced forms of privatized monitoring of individuals' life, fuelling what has been defined *surveillance capitalism*[5], a new form of capitalist accumulation centred around the exploitation and commodification of consumers' personal data. Whether from a public or corporate perspective, the unrestrained adoption of pervasive types of algorithmic surveillance, that are contributing to develop and shape the future of our algorithmic society[6], makes the equation "control of information" = "control of individuals" disturbingly accurate.

From another perspective, however, the notion of control acquires a completely different meaning, as it refers to the idea that individuals should have a level of control over the circulation of information relating to them, and should be able to participate in their governance. It identifies the multiple ways in which people have agency over their personal data and self-manage their sharing and use. In this respect, control over data becomes a form of *individuals' empowerment* rather than states or corporations' power.

The analysis carried out in this thesis develops and further explores this second interpretation. The idea of individuals having agency over data revealing information about themselves is embedded in the EU-based right to data protection and represents one of its characteristic features. While less dominant in the first European laws governing the processing of personal data, this idea of "individual control" has grown to be a central pillar of data protection acts around the EU. It is strongly attached to the view that in a society where information represents bits of one's "Self", in terms of identity and personality, being able to decide who this data is shared with and how it is used, is a fundamental expression of the rights of individuals to autonomy, identity, self-development and self-determination.

Despite the roots of the concept lie deep in fundamental rights-based considerations, very few examples exist in the international and European legal framework that expressly consider the right of individuals to participate and control their personal data

[4] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair: Balancing National Security and Data Protection' (2018) 56 JCMS: Journal of Common Market Studies 751.
[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (First edition, Public Affairs 2019).
[6] Oreste Pollicino and others (eds), *Constitutional Challenges in the Algorithmic Society* (1st edn, Cambridge University Press 2021).

as a general principle. As a matter of fact, only the international guidelines of the Organization of Economic Cooperation and Development (OECD)[7] clearly include a principle of "Individual Participation" among its provisions[8]. No other act is so explicit. Even the greatly-applauded General Data Protection Regulation (GDPR)[9] drops this concept of control only incidentally in one of its first recitals[10].

Lacking a general principle of this sort, data protection regulations have usually expressed the ideas of "control" and "participation" more obliquely, as a bundle of micro-rights that individuals should supposedly exercise to maintain agency and influence over the flow of their personal data, among which the ability to decide whether to share their personal data and to consent to their use for certain purposes. Individuals have a right to be provided with all information necessary to understand the processing activities and their possible consequences, in order to make free and conscious choices. Further, they are endowed with the means to oversee and, to a certain extent, influence the lifecycle of data that talk about them, even when these escape from their personal sphere (e.g., by accessing, rectifying, erasing or opposing to their uses made by third entities).

Over the last decade, the swift pace of information technologies and the new power dynamics of the digital ecosystem have undermined the ability of individuals to keep track, let alone manage, the streams of data they generate on a daily basis. This, in turn, has prompted EU Institutions and other privacy watchdogs to strongly voice the need to «put individuals back in control of their personal data»[11]. Empowering EU citizens to regain agency over their data has become a widely publicized goal of the 2016 data protection reform agenda, which, with the adoption of the GDPR, has worked

[7] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", adopted by the OECD in 1980.
[8] Par. 13, 1980 OECD Guidelines.
[9] 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).
[10] Recital 7 of the GDPR states: « […] Natural persons should have control of their own personal data».
[11] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (2012) COM/2012/09 final; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' (2010) COM(2010)609; Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (1 December 2009) WP 168.

to improve the ability of individuals to exert control, leading to an expansion of their subjective rights.

However, after three years into the GDPR, the feeling is that the much-revamped emphasis on data subjects' empowerment has so far been mostly barks and no bite. The little improvements that these manifold actions have been able to generate so far, in terms of awareness and influence that individuals can exercise when it comes to their data, keep raising tough questions on the effectiveness and feasibility of a "privacy self-management"[12] model.

Oftentimes, the ubiquity, vastity and complexity of the modern ecosystem of information leaves people overwhelmed and lost. Individuals are constantly overloaded with information, in a context where the network of intermediaries gathering, exchanging and using data keeps on growing without limits. Individuals are asked to understand and assess technologies that can be hardly comprehended by sector-specific experts. They are faced with choices, whose consequences they cannot fully grasp, and are increasingly exposed to the manipulations and influences of companies and entities that view them as goldmines.

Against these premises, the purpose of this work is to explore in depth the concept of "individual control" in the data protection realm, with a view to investigate its emergence in the EU data protection framework and its persisting shortcomings, and further attempt to examine what steps could be made to move forward, in order to offer the necessary support and supplementation to this principle.

The analysis takes as a primary reference the EU regulatory framework, even though references to national, international and extra-EU legal systems may be included, when deemed relevant for the purposes of the analysis.

The **First Chapter** introduces the concept of "individual control", exploring its origins and connection with data protection legislation, in Europe. After providing a brief overview of the scholars' debate around the notion of "control on personal data" in the context of the conceptualization of the right to data protection, the chapter investigates its emergence and materialization through its regulatory implementation. The analysis of the legal instruments regulating the processing of personal data that have been adopted

[12] The term "privacy self-management" has been taken from Solove's works, that uses it to indicate the ability of individuals to self-manage the privacy choices concerning their personal data. Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

over time attempts a comprehensive exploration at national, international and European level, starting from the early national statutes of the ‘70s, touching upon the Council of Europe and the OECD international instruments, up to the more recent GDPR. Finally, the chapter offers a quick overview of the relevant jurisprudence of the Court of Justice of the European Union on data protection-related cases, to determine whether CJEU case-law provide any additional insight into this concept.

The **Second Chapter** focuses on the major shortcomings that undermine the idea for individuals to exercise effective control over the circulation of their personal data, the aggravation of which goes hand in hand with the continued datafication of our society. In particular, the chapter explores the factors that contribute to the inefficiency of current individual control mechanisms offered by the EU data protection framework. These factors are grouped into three categories: (i) “cognitive”, when they refer to the human capabilities of understanding, reasoning and taking decisions; (ii) “systemic”, when they relate to exogenous causes connected to technological and structural changes in our society; and (iii) “legal”, when the enforcement fallacies depend on unclear legal interpretation and other practical complications.

In light of the numerous challenges that individuals face in the modern technological context, which translate into a general lack of control over the processing of personal data, the **Third Chapter** and **Fourth Chapter** seek to investigate what can be improved to restore individual empowerment and where other measures should instead be preferred to compensate for its insurmountable shortcomings.

The two final chapters attempt to analyse different mechanisms and approaches that, if adequately leveraged and applied, could offer effective support and complementation to the individual control model, with a view to increase the level of protection offered to individuals.

In particular, the **Third Chapter** focuses on a number of measures that have been defined “individual-centric”, as they aim at strengthening the control data subjects can exercise on their data, by essentially expanding the toolkit individuals are provided with to maintain agency over processing activities. Given the complexity and ubiquity of the modern data processing environment, however, the chapter highlights how providing individuals with enhanced technology-based instruments to exert their control rights is not alone sufficient to overcome some inherent limitations of human capacities.

The **Fourth Chapter**, therefore, expands the scope of the analysis and explores mechanisms and proposals that move beyond a strict “data subject-focused” dimension, in the sense that these measures, on the one hand, see as leading characters societal actors different than individuals alone and, on the other hand, approach data protection taking into consideration not only individual interests, but also collective and social ones. These measures are aimed at creating a broader “control” structure that should help to both to ensure that individuals are put in the proper conditions to exercise their rights effectively and consciously (thus they directly support the individual control model itself), and to supplement the protection gaps left by the individual control model, when it is inherently insufficient to stand against the threats that data processing activities may pose to individuals, groups and society at large.

CHAPTER I – The paradigm of "individual control" in the data protection framework

1 Introduction

The First Chapter investigates the emergence of the concept of "individual control over personal data" in a historical perspective, taking into account the doctrinal debate, regulatory interventions and most relevant case law on the matter.

After the main conceptual constructions of informational privacy and data protection are presented to offer a brief overview on the role assigned to the notion of "individual control" by the doctrinal debate[13], the chapter investigates the emergence and practical translation of this concept through its regulatory implementation. The analysis of the legal instruments adopted over time to govern the processing of personal data seeks to provide a comprehensive exploration that moves across the three national, international and European levels, starting from the early national statutes of the '70s, touching upon some relevant international instruments, up to the more recent EU General Data Protection Regulation.

In the absence of a generalized principle at EU level establishing a right of individuals to control the circulation of their personal data, the analysis focuses in particular on the different substantive measures that have been designed to enable individuals to exercise control over their data flows. Borrowing from Bygrave's terminology[14], these are referred to in the following chapter as "participatory" control mechanisms, namely measures/rights that individuals can directly enforce against data controllers[15] without the necessary intervention of an institutional body or other third parties. By way of contrast to this first category, and to better underline some of the adjustments and revisions to which data protection laws have been subject during time, the chapter maps also the other group of control measures laid down by these acts, that are referred to as "institutional" control mechanisms, which include measures that entrust third-parties, generally a supervisory authority, with specific authorization and monitoring powers.

---

[13] Although the research is conducted primarily from an EU perspective, the review of the doctrinal debate starts by reviewing the positions adopted by the US doctrine, considering the significance of the latter on the debate later developed in Europe.

[14] Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International 2002) 86.)

[15] According to EU data protection terminology, "data controllers" are subjects/entities that define the purposes and means of the data processing and are therefore the primary responsible for its correct performance.

Finally, against the doctrinal and regulatory background, the chapter looks briefly at the Court of Justice of the European Union jurisprudence, to examine whether the CJEU case-law can provide any additional insight on the concept of "individual control over personal data" and its connection to the right to data protection.

2 The role of "individual control" in the US and EU privacy and data protection debate

The notion of "control", as a form of empowerment of individuals over their information[16], is not new in privacy and data protection literature and it is, in fact, strictly related to the general debate around the conceptualization of these two rights. The genesis of this idea of "control over information" can be traced back to the flourishing doctrinal debate on privacy developed in the United States, country of origin of the notion of privacy itself. However, partly influenced by, partly independently from US positions, the concept of "control" has found a place of its own in European literature.

2.1 The United States' approach

Scholarly discussions on privacy in the US context started to develop around the early beginnings of the 20th century, following the first landmark definition of privacy as right to "be left alone" by scholars Warren and Brandeis[17]. According to this definition, privacy was conceived as a right to opacity and seclusion from intrusions in one's private sphere. A number of other interpretations followed this first one, prompting a lively debate over this new right to privacy in the following years[18]. This, however, has resulted in a general conceptual and doctrinal disagreement over the meaning of privacy and its underlying values (autonomy, intimacy, liberty), which still persists today, leading some authors to discard in whole the possibility of defining privacy as a unitary concept[19]. Despite its fluidity and extension, some leading trends of the debate, that chronicle the evolution of the notion of privacy and its connection with the concept of control, can be identified.

---

[16] Although "information" and "data" do not technically represent the same concept, this work employs the words interchangeably following the common and generalist understanding of the two notions.
[17] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[18] Colin J Bennett, 'Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s' (1991) 16 Science, Technology, & Human Values 51, 59.
[19] Daniel J Solove, *Understanding Privacy* (First Harvard University Press paperback edition, Harvard University Press 2009); Daniel J Solove, 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy* (Cambridge University Press 2015) <https://www.cambridge.org/core/product/identifier/9781107280557%23CN-bp-4/type/book_part> accessed 7 June 2021. However, although Solove argues privacy has different meanings and different functions, one of the "facets" of privacy is "control over personal information".

As mentioned above, initial theories described privacy primarily in terms of "being left alone" (non-intrusion theories)[20] or "being alone" (seclusion theories)[21], thus placing their focus on physical invasions in the private sphere. Both theories addressed in fact privacy concerns that pertained to physical access to individuals, through observation or unwarranted intrusion in one's space ("accessibility privacy") or, in a broader perspective, through interference in decision making processes ("decisional privacy")[22].

As a response to these first positions, other positions have moved away from physical intrusions and started to associate privacy with concerns on the flow of information, leading to the development of the expression "informational privacy"[23]. The latter are represented by two main theories, that share the focus for information-related privacy concerns, but differ for the way in which they construe the notion of privacy: the one in terms of "control", the other in terms of "limitation" (sometimes referred to also as "access").

Proponents of *control theories* claim that privacy is realized only when one has *control about the information concerning oneself*[24]. Different variations of this theory have emerged in US privacy literature, all united by the emphasis placed on the notion of "individual control". According to Westin, one of the most prominent names of this strand, privacy is the «claim of individuals [...] to determine for themselves when, how, and to what extent information about them is communicated to others»[25]. Miller describes privacy as «the individual's ability to control the circulation of information relating to him»[26]. Other authors have endorsed similar versions of the control theory, like Fried, who recognizes that privacy «is not simply an absence of information about

[20] One of the most prominent examples of this theory is certainly provided by the seminal article of Warren and Brandeis. Warren and Brandeis (n 17).
[21] A variation of the seclusion theory is endorsed, for example, by Gavison as he describes privacy as the being «completely inaccessible to others», Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 428. Another version is supported by Warren and Brandeis themselves, when they define privacy as the necessity of individuals to "retreat from the world" Warren and Brandeis (n 17) 196.
[22] "Accessibility" would concern physical access through observation or in the form of unwarranted intrusion into one's person through someone physically accessing one's personal papers. "Decisional" would concern factors or actions that interfere with an individual's ability to make certain kinds of decisions. See further, Herman T Tavani, 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy' (2007) 38 Metaphilosophy 1, 6.
[23] ibid 7.
[24] The most prominent authors who have advocated for some kind of version of the control theory of privacy over the years include: Alan F Westin, *Privacy and Freedom* (Atheneum 1967); Arthur R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Univ of Michigan Press 1971); James Rachels, 'Why Privacy Is Important' (1975) 4 Philosophy & Public Affairs 323; Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 475.
[25] Westin (n 24) 7.
[26] Miller (n 24) 125.

us in the minds of others, rather it is the control over information we have about ourselves»[27] and Rachels, who stresses the social dimension of privacy arguing it depends on the connection between «our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships»[28]. The control theory places great emphasis on the individual and the role of his *choice* in granting or denying access to personal information. Critics of this theory contest its lack of clarity regarding the type of data on which one can expect to have control and the extent of such control[29], as well as the inconsistency arising from the fact that even in cases of complete control a lack of privacy could still exist[30]. Despite these criticisms, "privacy control theories" keep on being endorsed even by more recent commentators dealing with the contemporary issues posed by digital technologies[31].

On the opposite side, advocates of the *limitation* (or access) *theory* frame the privacy discussion in terms of *restrictions over access to information in certain context*[32]. According to this theory, informational privacy is described as a «limitation of others' access»[33] to individual information or as a «condition of not having undocumented personal knowledge about one possessed by others»[34]. While the merits of this theory were recognized in the definition of geographical boundaries, in terms of specific "zones" (contexts) of privacy[35] in which restrictions to access could be imposed, critics underlined the theory failed to appreciate the importance of control in constructing this zone and the role of the concerned person to grant or deny access to it[36].

---

[27] Fried (n 24) 482.
[28]Rachels (n 24) 326.
[29] Tavani (n 22) 6–7; David W Shoemaker, 'Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity' (2010) 12 Ethics and Information Technology 3, 3.
[30] Tavani offered the example of a person that willingly decided to disclose each piece of himself to the world by publishing any information on a public website and installing CCTV cameras in every room of the house, Tavani (n 22) 8. Shoemaker approaches the same argument stating that one's privacy ranges over a specific domain of generally unrevealed information, and one has privacy to the extent one exercises control over access to that domain. Consequently, if there is simply no unrevealed personal information left over which one could exercise control, one would have no privacy left either. Shoemaker (n 29) 3.
[31] See for a brief overview of more recent trends, Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 SCRIPTed 7 <http://script-ed.org/?p=1927> accessed 7 June 2021.(7).
[32] See e.g., Gavison (n 21); William A Parent, 'Privacy, Morality, and the Law' (1983) 12 Philosophy & Public Affairs 269.
[33] Gavison (n 9) 4.
[34] Parent (n 32) 269.
[35]Tavani (n 22) 10.
[36] Shoemaker (n 29) 3.

The issues arising from these theories prompted the development of a third hybrid theory (called the *Restricted Access/Limited Control theory*, "RALC"), which was supposed to *merge the strengths of the above-mentioned theories* into one[37]. According to this theory, one has privacy to the extent one is protected «from intrusion and information access by others in the context of a situation»[38], namely when there is normative zone (i.e., a conventional, legal, or ethical norm) limiting access to information in certain contexts[39]. However, "limited control" plays a role in the justification of these norms (i.e., restrictions are erected to provide individuals with some control over certain information) and in the management of one's information (i.e., in cases one is allowed to waive these restrictions)[40]. Blind spots of this theory were identified in its vagueness to provide a clear way to handle privacy in public and its excessive concerns over the "context" in which information is accessed rather than the "type" of information[41].

Conceptual discussions about the meaning of privacy and the role of individual control in US literature were influenced and conflated with the debate around the values underlying privacy (e.g., autonomy, personal liberty), as its normative underpinning[42]. Depending on the overarching value taken into consideration, the function and prominence that the notion of control was conferred in the theoretical construction has varied.

It is not the purpose of this paragraph to dwell further on the theoretical discussion that still inflame the multifaceted privacy debate in the US, however the brief overview above is sufficient to appreciate the key role that "control over one's information" plays in the information privacy discourse, regardless of the perspectives chosen. This is quite evident in the *control* and *RALC theories*, but, as it was noted[43], an element of individual control concerns unavoidably also *limited theories*, where it translates in the power of the individual to limit other's access into one's private space. As clarified in the next

[37] The RALC theory was developed by Moor and Tavani in a series papers. See James H Moor, 'Towards a Theory of Privacy in the Information Age' (1997) 27 ACM SIGCAS Computers and Society 27; Herman T Tavani and James H Moor, 'Privacy Protection, Control of Information, and Privacy-Enhancing Technologies' (2001) 31 ACM SIGCAS Computers and Society 6; Tavani (n 22).
[38] Tavani (n 22) 12.
[39] Shoemaker (n 29) 4.
[40] Tavani (n 22) 12.
[41] Shoemaker (n 29) 12.
[42] Different values have been identified as conceptual underpinnings of informational privacy, see e.g., Helen Nissenbaum, 'Toward an Approach to Privacy in Public: Challenges of Information Technology' (1997) 7 Ethics & Behavior 207; Shoemaker (n 29) 7–14.
[43] Lazaro and Le Métayer (n 31) 15.

section, the US concept of “informational privacy” does not perfectly translate into the modern European concept of “data protection”, given the different construal paths that the rights followed in the two continents, as well as the different substantive underpinning values that US and EU literature have linked to the emergence of these rights[44]. As a consequence, neither the meaning assigned by US literature to “control over information” perfectly overlaps with the European understanding. However, the pioneering discussion in the US continent have undoubltly played a role in shaping the European debate, emerged only in subsequent years.

2.2 The European approach

The emergence of the concept of privacy in Europe followed different routes, in light of the very diverse historical and constitutional traditions of European national states. In Italy, for example, the absence of a normative foothold that could ground a right to privacy (“riservatezza”) had sparked a long-standing debate among Italian scholars on the recognition of this right in the Italian legal system[45]. The debate was ended by the Italian Supreme Court in 1975[46], when it formally established that the Italian legal system recognized a right to “riservatezza”, understood as the protection from interferences of «situations and events strictly personal and familiar» even if occurred outside the domestic domicile, as a particular aspect of a general right to personality enjoyed by all citizens stemming from Art. 2 of the Italian Constitution[47].

Whether named “*riservatezza*”, “*viè privèè*” or “respect for private life”, the initial interpretation of privacy resembled the US seclusion view according to which privacy was understood as a right to “opacity” that protected the intimacy of one’s private sphere against outside intrusions[48]. The progressive expansion of the notion of privacy, as a reaction to the rise of technological developments that left individuals vulnerable in new ways thanks to the ever-growing use of their personal information, lead to the materialization of a new concept in the European landscape, entirely concerned with the processing and circulation of personal information: “data protection”. This concept is

[44] Orla Lynskey, *The Foundations of EU Data Protection Law* (First edition, Oxford University Press 2015) 178.
[45] Stefano Rodotà, *Elaboratori Elettronici e Controllo Sociale* (Il Mulino 1973) 127–128.
[46] Italian Court of Cassation, 27 May 1975, n. 2129 in Mass. Giur. It., 1975, 594.
[47] Art. 2 of the Italian Constitution states «the Republic recognises and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed».
[48] 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?* (Springer Netherlands 2009) 63.

often associated with the US notion of "informational privacy", which in a similar fashion focuses on issues linked with personal information flows. However, although the theoretical constructions behind the US version had an undoubtful influence on the European developments and some similarities between the two concepts exist, these remain very distinct. One of the most apparent differences is that data protection applies to a broader range of data processing activities and grants individuals more rights over this broader range of data[49]. Also, the contextual use of the term "control" does not always overlap. In US theoretical constructions, "control over information" has traditionally been associated with the ability of a person to control the "access to" or the "collection of" their information, therefore mainly focusing on the first phase of data disclosure. On the contrary, the European notion has been notably broadened to encompass monitoring powers over the entire lifecycle of personal data, even when data are no longer in the "domain" of the data subject.

Likewise in the US, however, the rationale of this "new" European right remains a highly disputed matter. As extensively explained in the following paragraphs, the history of the right to data protection is very peculiar: from the '70s it made its first appearance in early national laws governing data processing, where it was conflated or linked at different levels with the right to privacy; in 1995 it was essentially translated into a secondary EU instrument, where the connection with privacy and other fundamental rights grew stronger; and only very recently, in 2009, it achieved the status of autonomous fundamental right in the Charter of Fundamental Rights of the European Union. As a result of this tortuous path, the emergence of the right to data protection has never been interpreted univocally. Despite the different reasons advanced by European scholarship, there is still no unanimous conclusion on a coherent explanation for the introduction of a self-standing (fundamental) right to data protection, neither on the distinctive traits and underlying values of this right compared to the well-established right to privacy[50].

According to Lynskey, existing literature has construed the relationship between privacy and data protection based on three different models. The latter have not developed completely unrelated and have influenced each other in various ways, also in light of the evolving European regulatory and jurisprudential background marked by a number of

[49] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 11.
[50] ibid 91–93.

ground breaking events (like Convention 108; Directive 95/46/EC or 1983 German Population Census decision). Some distinctive features, however, key features can be traced for each model.

Under the first model, data protection and privacy are viewed as intermediary tools which serve the ultimate goal of ensuring the respect of individual personality, as a direct derivation of human dignity[51]. Human dignity, together with its articulations, in particular self-determination, is therefore chosen as the conceptual foundation for the right to data protection[52]. Authors endorsing this model considers «control over personal information about oneself one projects into the world» a distinctive feature of data protection, opposed to the «freedom from constraints in the construction of one's personality», typical of the right privacy[53]. However, they also believe that "inclusion and participation", on one side, and "seclusion", on the other, are two facets of the same medal. Despite pursuing complementary normative goals, in fact, privacy and data protection share a common normative justification in the promotion of human dignity in terms of human personality, both as individual self-determination and decisional autonomy[54].

The second model sees data protection as the most recent evolution of privacy, initially conceptualized as seclusion and now evolved to encompass elements of informational control[55]. According to this view, the differences existing between data protection and privacy are the result of the progressive transformation and expansion of the latter due to technological changes. However, the objectives served by data protection remain the same as privacy. Rodotà embraces this position as he states that «privacy is also to be understood as "the right to keep control over one's own information and determine the manner of building up one's own private sphere"»[56]. He recognizes that the distinction between the right to respect for one's private and family life (privacy) and the right to the

[51] Notably, Lynskey mentions the famous 1983 Population Census Decision (see *infra* par. 3.2), in which the German Constitutional Court recognized the right of individuals to determine for themselves the disclosure and use of their data, as a particular ramification of the right to personality, itself stemming from human dignity. ibid 95.
[52] ibid.
[53] Rouvroy and Poullet (n 48) 75.
[54] ibid 76.
[55] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 101–102.
[56] Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 76; Stefano Rodotà, *Tecnologie e Diritti* (Il Mulino 1995) 101.

protection of personal data «is more than an empty box»[57] and reflects the journey that led the latter to evolve and drift away from the former. The right to privacy, in fact, mirrors a "static and negative kind of protection" to prevent others from interfering from one's private life. Data protection, on the contrary, confers a "dynamic protection" as it sets out rules and empowers one to take steps[58]. However, to demonstrate the fragile and flexible boundaries of these different conceptual models, Rodotà echoes the "human dignity" model and asserts the existence of a strong link between the achievement of individual's dignity, autonomy and self-determination, and the right to data protection.

Finally, according to a third view, data protection is construed as an independent right. According to these scholars[59], even though data protection has significant overlaps when "data privacy" is concerned, it has different foundations from the right to privacy. They believe approaching data protection from this perspective is more respectful of the distinctive constitutional traditions of EU states[60]. For example, while the Netherlands and Belgium have linked data protection to privacy from the beginning; France and Germany anchored it to different rights: the former on liberty; the latter on the recognition of human dignity[61]. Endorsing a version of this model, De Hert and Gutwirth claim that privacy and data protection should be seen as two distinct legal tools that perform different but complementary functions[62]. Privacy, conceived as a tool of *opacity*, is concerned with the establishment of limitations to power (rules of non-interference); data protection, as a tool of *transparency,* is concerned with controlling and channelling the accepted exercise of power[63]. Others such as Tzanou, instead, argue that for the right to data protection to operate independently from privacy it needs to be construed as acting both positively (control power) and negatively (prohibit power), although she

[57]Rodotà, 'Data Protection as a Fundamental Right' (n 56) 79.
[58] Rodotà, *Tecnologie e Diritti* (n 56) 102–108.
[59] See e.g., Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222; Maria Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014); Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the criminal law* (Intersentia 2006).
[60] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 103–104.
[61]P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 9–10.
[62] De Hert and Gutwirth (n 59) 62.
[63] ibid 70.

acknowledges it may not be “mature” enough, as it currently stands, to operate alone[64]. The main point of this model is to emphasize the multifaceted function of data protection. This right serves in fact different values, besides privacy, and pursues a range of other objectives, which find expression in a series of principles, among which the “individual participation and control” one[65].

Regardless of the specific model one choses to adhere to, therefore the relationship between data protection and privacy upheld, across European doctrinal discourse “control over personal information” appears to be recurrent trait associated, in some way or another, to data protection. Whether as an attribute emerged from the evolution of the right or as one of its native properties, “control” and “individual participation” are unanimously recognized as added values or, more correctly, distinctive features of data protection. Therefore, despite many differences persist in the conceptual understanding of data protection, EU scholarship seems to generally have elected this principle as one of the conceptual underpinnings and characteristics facets of data protection. In line with the human rights-based construction of the European right to data protection, the type of control individuals should be able to exercise over information relating to their identity and personality embodies a key expression of those core values on which data protection has been variously grounded, each of which entails a level of individual agency and self-determination.

However, as clarified in the next paragraphs, while the emphasis on individual control and personal data has exponentially grown at both doctrinal and institutional level, the strict connection between data protection and active engagement of individuals was not as present when this right first emerged in Europe. From a regulatory perspective, in fact, the idea of individual control did not play a central role into the first national informational privacy/data protection laws that emerged in Europe in the early ‘70s, or at least it was not as apparent. The attention placed on individual control over the processing of personal data, as an inherent and instrumental component of data protection, and its affirmation into the growing introductions of subjective rights conferring authoritative powers to individuals has become part of institutional discussions and was further translated into legal instruments in a gradual way.

[64] Tzanou (n 59) 87.
[65] ibid 90.

3 Early national frameworks (1970-1995)[66]

Since the 1970s European countries started to adopt laws to govern the collection of personal data and their automated processing. The German Federal State of Hessen and Sweden were the two countries to open the first season of data protection laws, and were followed in subsequent years by an increasing number of European states. With a view to understand how the concept of individual control emerged and translated in legal acts, since the origins of data protection in the EU, this paragraph provides an overview of the early regulatory interventions in this field, covering almost three decades of history, starting from the 70's until the mid 90's, before the implementation of the first harmonized initiative at EU level, Directive 1995/46/EC.

The analysis that follows draws inspiration from Schönberg's comparative study of domestic data protection laws, which follows a "generational approach" and groups data protection norms by similarities of data protection regimes[67]. Even though the generational model requires some approximation and categorization that may result into improper generalization[68], the grouping exercise is useful to highlight some notable trends during the years. Acknowledging its limits and the existence of different exceptions and national peculiarities, the groups of norms should thus not be considered fixed chronological blocks, rather stretching categories that may in some instances overlap on one another.

Below a schematic timeline of the different data protection acts that are analysed hereinafter.

[66] All translations of national laws contained in this work are based on English translations available at https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic, in Council of Europe, *Legislation and Data Protection : Proceedings of the Rome Conference on Problems Relating to the Development and Application of Legislation on Data Protection* (Camera dei Deputati 1983); and on self-made translations of the original documents made with translation software.
[67] Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press 1997).
[68] Bygrave (n 14) 88.

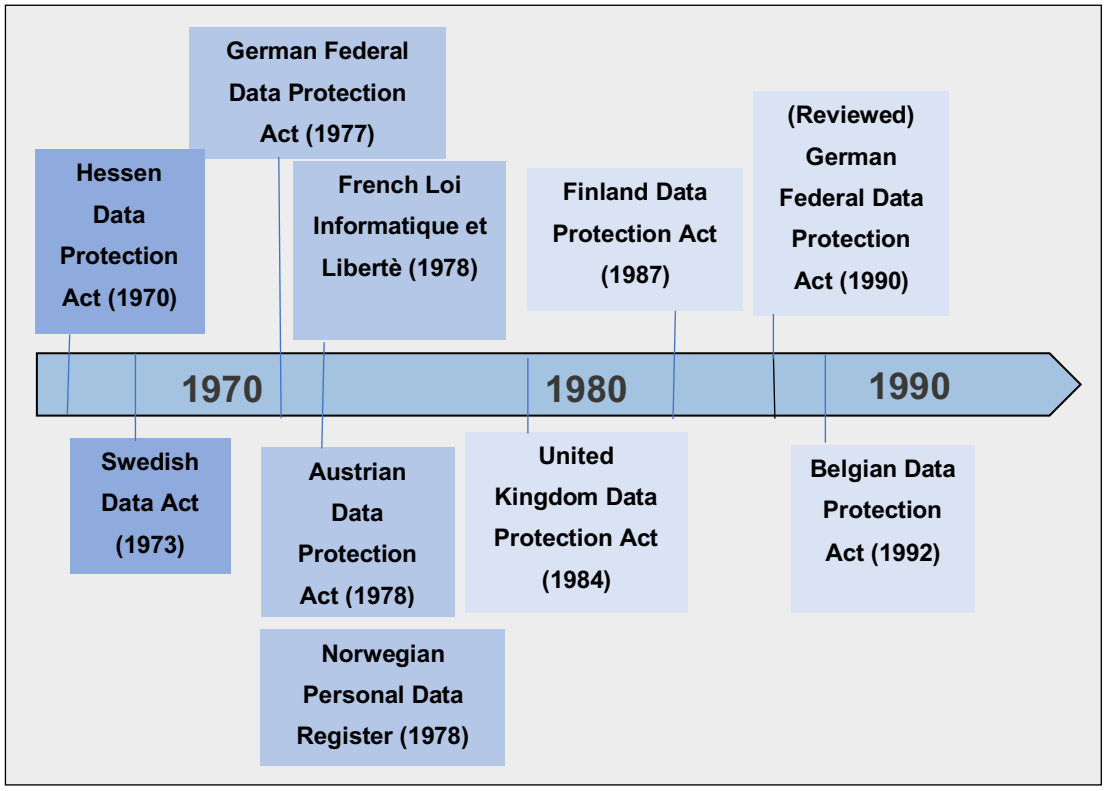

Table 1. Timeline of national data protection acts (1970 – 1995)

3.1 The forerunners of technology regulation (early 1970s)

BACKGROUND - The pioneering legislations in Europe that regulated the processing of information related to individuals date back to the early 1970s'. The Data Protection Act of the German state of Hesse (the "*Hessische Datenschutzgesetz*", 1970)[69], considered the first independent "data protection" law in Europe, and the Swedish Data Act ("*Datalag*", 1973)[70] fall in this first wave of norms.

[69] *Datenschutzgesetz* (GVBl. II 300-10) vom 7. Oktober 1970. Other German federal states had adopted some provisions to govern data processing, but they were mostly norms incorporated in legal acts regulating other subject matters. The Hessen Data Act was therefore the first separate and independent law to expressly regulate data processing activities. Frits W Hondius, *Emerging Data Protection in Europe* (North-Holland Pub Co ; American Elsevier Pub Co 1975) 35.

[70] *Datalag* (1973:289), Svensk författningssamling, 11.05.1973. According to Mayer-Schönberg, there are three main "generations" of data protection laws. According to the author, the "first generation" includes, beside the ones mentioned above, also the data protection statute of Rheinland-Pfalz (1974), the Austrian proposals for a data protection act and the German Federal Data Protection Act (1977). Mayer-Schönberger (n 67) 221. Due to their language and structure, however, it seems these acts are closer to the "second generation" of statutes rather than the first one, and will be therefore dealt within the next paragraph. Other scholars, instead, consider that the first wave of data protection laws covers the period until the adoption in 1981 of Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"). González Fuster (n 59) 56 quoting ; Spiros

These first-generation statutes represent a reaction to technological developments and a direct response to citizens' resistance to centralized national data banks[71]. Two were the main drivers that led to the enactment of data processing norms: pervasive technological changes and public fears over their possible consequences. The advent of informatization and the deployment of the first massive computers determined a decisive growth in the capacity to collect, store, and exchange identifiable information about individuals[72]. At the same time, the economic and social reforms initiated in all Western European nations since the '60s were demanding increasing amounts of citizens' information to enable governments to plan, administer and manage new policy measures[73]. Recently developed technical abilities and growing pressure to build usable data gatherings resulted in the creation – or at least proposal – of centralized national information banks. In particular, in German, the Hessian state administration promoted the establishment of central data processing facilities to help public authorities to access and use information of citizens for policy making decisions[74]. Around the same time, Sweden conducted a population census and suggestions were made to merge census data with registration and tax records into one national information bank[75]. These developments, however, sparked a fiery public debate over the risks of governments' surveillance capabilities and dehumanized bureaucratic procedures[76], raising citizens' fears of a Big Brother society and robotized administration[77]. While public concerns were particularly focused on the new possibilities for governments to invade and control citizens' lives, the same technological shift was taking place, at an ever-increasing pace, also in the private sector. Large business corporations were exploring the potential of computerization and mass data collections to enhance their organizational, management and business capabilities[78], equally threatening citizens' privacy[79].

Simitis, 'Einleitung: Geschichte—Ziele—Prinzipien' in Spiros Simitis and others (eds), *Bundesdatenschutzgesetz* (Nomos-Verl-Ges 2011).

[71] Hondius (n 69) 2–6.

[72] David H Flaherty, 'Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies' (1986) 11 Science, Technology, & Human Values 7, 7.

[73] Mayer-Schönberger (n 67) 222.

[74] Hondius (n 69) 5; Spiros Simitis, 'Zwanzig Jahre Datenschutz in Hessen - Eine Kritische Bilanz' (1990) 19 Tatigkeitsbericht des Hessischen Datenschutzbeauftragten 138, 69; González Fuster (n 59) 57.

[75] David H Flaherty, *Privacy and Government Data Banks: An International Perspective* (Mansell 1979) 105.

[76] Mayer-Schönberger (n 67) 222–223.

[77] Hondius (n 69) 3; Flaherty, 'Governmental Surveillance and Bureaucratic Accountability' (n 72) 8; Bygrave (n 14) 100–104.

[78] Mayer-Schönberger (n 67) 222–223; Bygrave (n 14) 96–98.

[79] Hondius (n 69) 7 and on the Swedish Data Act 46.

To soothe the generalized aversion to centralized information banks and automated data processing more generally, States responded by adopting rules that laid down limits and conditions to automated data processing. Even if these first rules were mainly addressed to govern the public sector's uses of personal data, similar measures started to applied also to private entities[80].

OBJECTIVES - These first data acts took mainly a "functional outlook" to data processing[81], or in Bennet's words a "technology-control" approach[82]. The problem was identified as essentially a technological one, which led to solutions framed in the shape of rules governing data quality and technical safeguards[83]. This approach was not concerned with the relationship between the individual and his personal data, instead it concentrated its efforts mainly on regulating technical aspects connected to the use of computers and the processing of information. In a pioneering fashion, the Hessen Data Protection Act was the first act in Europe to include a section titled "*Datenschutz*"[84] (data protection), however the section wording suggests that the term was employed mainly in descriptive terms, to group a set of rules that governed data storage and transmission[85], with no particular connection to individual rights. While the protection of individuals was presented as one of the underlying purposes of these acts[86], the rules and structure of these first norms appeared primarily aimed at safeguarding the collectivity from societal threats posed by the misuse of personal information and ensuring compliance with the general values of society, rather than protecting individual interests[87].

MAIN PROVISIONS - This technology-oriented approach can be traced back to a number of elements. First the language used by these statutes. They privileged

[80] The Hessen Data Protection Act regulated only automated data processing in the public sector, the Swedish Data Act contained instead provisions that addressed both the public and private sector.
[81] Mayer-Schönberger (n 67) 223.
[82] Bennett (n 18) 56–57.
[83] ibid.
[84] Section 1 of the Hessen Data Protection Act.
[85] González Fuster (n 59) 57.
[86] The Hessen Data Protection Act did not contain any express provision in these terms, however, according to Simitis, its purpose was indeed to protect individuals against the potential dangers of automated data processing. See Council of Europe (n 66) 18. Despite the absence of a general provision on the objectives of the Swedish Data Act, the rules referred to the prevention of undue invasions of the personal integrity of the person (*iregistrerads personliga integritet*), whose data were registered in data banks. González Fuster (n 59) 59.
[87] Mayer-Schönberger (n 67) 223.

technical terms, such as "data", "files", "records" and "data bank"[88]. Further, these statutes provided for the most part general obligations that required data handlers (i.e., the later "data controllers") to act in a certain way and adopt certain safeguards. The Hessen Data Act laid down the primary conditions for legitimate data processing, which included mainly confidentiality and security rules that data controllers needed to observe[89]. Along the same lines, the Swedish Data Act contained express provisions on information accuracy and related duties of correction and completion[90], restrictions upon dissemination and secrecy obligations[91].

PARTICIPATORY CONTROL - The functional attitude of these laws echoed the role they reserved to individuals. No general principle or provision on subjective control and participation was included in these first-generation acts and very few and marginal individual rights were present. Access rights were not introduced in favour of individuals, rather legislative bodies, to counter-balance the centralization of informational powers in the hands of the executive bodies and enable parliaments to request from central administrations the disclosure of citizens' data[92]. Consent, as an authorization mechanism to collect and process personal data, was not envisaged[93]. Individuals could exercise a small set of subjective rights. The Hessen Data Protection Act included a right to rectify and block further data processing[94] and a general right to complaint

[88] ibid 224.
[89] In particular Sections 2, 3(1) and 5(2) of the Hessen Data Protection Act required public authorities to obtain, transmit and store data, record or files in such a way that they could not be consulted, altered, extracted or destroyed by an unauthorized person and prohibited from communicating or making them available to unauthorized persons. Hondius (n 69) 35; González Fuster (n 59) 57.
[90] Section 8 and 9 of the Swedish Data Act.
[91] Sections 11 and 13 of the Swedish Data Act. See in particular, Jan Freese, 'The Swedish Data Act' (1977) 178 Current Sweden 4..
[92] Section 6 of the Hessen Data Protection Act.
[93] Section 3 of the Hessen Data Protection Act ("Data secrecy") did include a reference to "consent", however it was referred not to the individual concerned (data subject), rather to the authorization of the "responsible to exercise control over records", necessary for the further communication of the information concerning the records. Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013) 43 and 47. It should also be noted that these acts were mainly addressed to public bodies and public sector data processing. A lack of individual consent was not therefore too surprising. However, the absence of consent is relevant in the Swedish Data Protection Act, which addressed not only public sector activities (where overriding public interests may well outweigh individual consent) but also private sector's data processing.
[94] Section 4(1) of the Hessen Data Protection Act included the right to demand the rectification of incorrect data («*sind gespeicherte Daten unrichtig, so kann der Betroffene Berichtiguag verjangen»*), while section 4(2) enabled any person whose rights were infringed by unlawful access, alteration, destruction or extraction («*widerrechtliche Hinsicht, Anderung oder Vernichtung oder durch einen widerrechtlichen Abrufœ»)* to demand that such action be discontinued if there was a danger of further infringement.

before the Data Protection Commissioner[95] (i.e., the established supervisory authority). The Swedish Data Act, instead, provided a limited information obligation for data controllers to provide details on the processing, upon request of the concerned subjects and only under certain conditions[96]. In any case, these few rights seemed to have essentially a "functional role", namely their exercise contributed to achieve better quality and accuracy of the information processed, rather than serving as "control tools" of the individual[97]. In essence, rules that regulated the use of technology took precedence over the protection of individual privacy rights[98].

INSTITUTIONAL CONTROL – Whereas individuals had a relatively passive role, these acts placed greater weight on institutional control mechanisms. The earliest supervisory authorities, the Hessen Data Protection Commissioner (*Datenschutzbeauftragter*)[99] and the Swedish Data Inspection Board (*Datainspektionsnämnden*)[100], were born with these first-generation acts, entrusted with monitoring tasks to ensure compliance with data protection rules and investigative powers to perform their functions[101]. A distinguishing feature of the Swedish Data Inspection Board was its responsibility to assess and authorize incoming submissions for data processing operations[102]. The Swedish Data Act provided, in fact, for a structured licensing scheme according to which each computerized personal register could be created or kept only with the permission and at the conditions set by the appointed national authority[103].

	Interests protected	Participatory control	Institutional control
Hessen Data Protection Act (1970)	Not explicitly stated	- Right to rectification and update - Right to appeal and	- Supervision by Data Protection Commissioner

[95] Section 11 of the Hessen Data Protection Act.
[96] Section 10(1) of the Swedish Data Act provided that at the request of a registered individual, the keeper of the register had to inform him of the personal information concerning him recorded in the register and that new information did not to be given up to twelve months later. See Freese (n 91) 4.
[97] González Fuster (n 59) 59; Flaherty, *Privacy and Government Data Banks* (n 75) 112.
[98] Mayer-Schönberger (n 67) 225.
[99] Section 7 and ff. of the Hessen Data Protection Act.
[100] Section 15 Swedish Data Act.
[101] Section 10 of the Hessen Data Protection Act and Sections 15 – 16 of the Swedish Data Act. See Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992) 166.
[102] Hondius (n 69) 44.
[103] This was provided by section 2 of the Swedish Data Act. Upon request of the register's holder, the authority initiated a complex assessment process that was meant to evaluate whether the personal register could lead to an «undue encroachment on the privacy of individuals». At the end of the assessment, the authority could grant a permission conditioned by specific directives. See Rodolfo Pagano, *Panorama of Personal Data Protection Laws* (Camera dei Deputati 1983) 78–79.

		restoration	
Swedish Data Act (1973)	- Personal integrity	- Right to information (obligation to provide information)	- Prior authorization of the Data Inspection Board - Supervision by Data Inspection Board

Table 2. Data protection acts 1970-1973

3.2 From technology-control to individual liberty (1975 – early 1980s)

BACKGROUND - While the first data acts focused on massive (usually public) data banks, in less than a decade, bulky and expensive computers were replaced by manageable and user-friendly "microcomputers"[104]. The power to collect and process information was not only amplified, it was decentralized[105]. Small businesses and individuals could have the same processing and monitoring capabilities of public bodies and large corporations. Old procedures (like the Swedish licensing scheme) became too elaborate and time consuming to keep up with this expansion process[106] and individuals started to want to be more actively involved in the circulation and processing of information concerning them[107]. These changes contributed to shift the approach to automated data processing issues, from a "technology" oriented perspective to one in which "individual rights" gained increasing consideration[108]. This thematic re-orientation is visible in data protection acts adopted in the second half of the 70s', including the German *Bundesdatenschutzgesetz (BDSG)*[109] of 1977; the French *Loi Informatique et Libertè*[110], the Austrian *Datenschutzgesezt*[111] and the Norwegian *Lov om personregister*[112], the last three all adopted in 1978.

OBJECTIVES - The individual rights turn became apparent under a number of aspects. Technical language left the place to broader and technology-neutral definitions and

[104] Bennett (n 18) 53–54.
[105] Bygrave (n 14) 95–96; Bennett (n 18) 54.
[106] See Corell in Council of Europe (n 66) 110 and 121–122.
[107] Mayer-Schönberger (n 67) 226–227.
[108] Bennett (n 18) 58.
[109] *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* (*Bundesdatenschutzgesetz* – BDSG) vom 27. Januar 1977, in der Fassung der Bekanntmachung vom 1. Februar 1977 (BGBl. I Nr. 7 S. 201).
[110] Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[111] Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG). BGBl. Nr. 565/1978.
[112] *Lov om personregistre m.m*. (LOV-1978-06-09-48). Among all the acts, the Norwegian one

terms[113] and fundamental rights of individuals started to be mentioned as a primary purpose of protection. The French *Loi Informatique* explicitly stated that information technology could not undermine «human identity, human rights, privacy, or individual or public freedoms»[114]. Section 1 of the Austrian DSG provided that everyone had «the right to confidentiality of personal data concerning him», particularly «with regard to respect for his private and family life»[115]. Even the BDSG, quite elusively, claimed that the purpose of data protection was «to prevent harm to any personal interests that warrants protection»[116]. There was no shared alignment across European countries on which values these rules were aimed at protecting[117], whereas the term "data protection" was rarely mentioned and remained a vague concept, although its link with individual rights was further strengthened.

MAIN PROVISIONS - The technology-control outlook does not disappear. Data protection norms adopted or updated during this second period still contained a robust set of provisions that focused on "data" and "data processing", laying down obligations and requirements that data handlers needed to comply with. The BDSG set forth a number of conditions for data processing[118], provisions on data secrecy and data security[119], specific storage and transmission obligations for processing in the public and private sectors[120]. The *Loi informatique* included fairness and lawful principles of data collection[121]; it imposed restrictions on data storage and introduced security obligations[122]. The implementation of technical and organizational measures was a

[113] Mayer-Schönberger (n 67) 226.
[114] Article 1 of the Loi Informatique et Libertè.
[115] This is also one of the unique cases in which a regulation mentions a "*Grundrecht auf Datenschutz*", a "fundamental right to data protection", although the concept is not further expanded on.
[116] § 1, BDSG. Although the wording is quite broad, according to Odermann "personal interests that warrant protection" was to be considered an alternative expression for the phrase "the right of privacy". J Lee Riccardi, 'The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?' (1983) 6 Boston College International and Comparative Law Review 243248 quoting; Hans-Joachim Ordemann and Rudolf Schomerus, *Bundesdatenschutzgesetz: BDSG* (5. Aufl, Beck 1992) 31–32.
[117] For a comprehensive overview of the interests and values safeguarded by data protection laws see Bygrave (n 14) 125–143.
[118] § 3 BDSG, titled "Permissibility of data processing" ("*Zulässigkeit der Datenverarbeitung*"), Riccardi (n 116) 58.
[119] § 5 ("*Datengeheimnis*," Data secrecy) and § 6 ("*Technische un organisatorisce Maßnamen*", Technical and Organisation measures) of the BDSG.
[120] Provisions distinguished between data processing in the public sector (sections 9,10, 11 of the BDSG) and in the private sector (sections 23, 24, 32). Riccardi (n 116) 252–257 and 261–264.
[121] Article 25 of the French *Loi Informatique* prohibited the collection of data in a fraudulent, unfair or illicit manner.
[122] *Ibid*, Articles 28 and 29 imposed that "nominal information" should not be stored longer than initially foreseen and always kept under strict security conditions.

requirement also in the Austrian DSG[123] and of the Norwegian Personal Register Act, both of which and included specific correction and deletion obligations[124] [125] for incorrect and irrelevant data.

PARTICIPATORY CONTROL - This second-wave of acts expanded the active involvement of individuals in the collection and processing of their data and introduced a number of substantive rights. The right for the data subject to receive information about the processing of his data became a solid presence in these regulations: the BDSG[126], the French Law[127], the DSG[128] and the Norwegian one[129] all contained a right to information, framed mostly in the form of what should now be a modern right to access (namely information was provided only upon subjects' request). This right was further supplemented by other individual rights, such as the right to correct and supplement existing information[130] or the right to block the use of data due to suspicions of inaccuracy[131]. In an innovative fashion, the French law granted data subjects with a right to "know and contest" the reasoning used in automated processing whose results could be used against them[132]. Individuals' consent started also to surface as a data collection requirement. In some cases, consent became a precondition to data processing[133], in other cases an "opt-out" regime was in introduced, based on which individuals could oppose to certain processing activities[134] or data transfers[135].

---

[123] Austrian DSG § 10 (*Betriebsordnung*) for public bodies and § 20 ("*Datengeheimins*") and § 21("*Datensicherung*") for private bodies. These provisions prescribed the implementation of adequate technical and structural measures.
[124] § 12 and § § 26-27 of the Austrian DSG.
[125] § 8 of the Norwegian Personal Register Act.
[126] § 4(1) of the BDSG, under the "Right of the data subject" umbrella.
[127] Article 27 of the *Loi Informatique*, that listed also the information to be provided to concerned individuals.
[128] § 11 and 25 of the DSG introduced a right to information that public/private entities had to comply with upon request and proof of identity. More specific information obligations were also included in § 22 of the DSG.
[129] § 7 and § 20 (specific for entities providing credit information services) of the Norwegian Personal Register Act.
[130] Articles 34, 35 and 35 of the *Loi Informatique*; § 4 (2) BDSG. Further specifications of these rights were included in the sections of the BDSG dedicated to data processing in the public and in the private sector.
[131] § 4(3) BDSG.
[132] Article 3 of the *Loi Informatique*. See González Fuster (n 59) 65.)
[133] § 3 of the BDSG, that laid down the conditions for data processing, including the "written consent" of the concerned person as one of the two legal grounds for a legitimate processing. See ibid 49–59.
Under the Norwegian Personal Register Act, in the context of processing related to opinion polls and market surveys, § 33 stated that: «data concerning name, date of birth, may not be entered into a filing system without the consent of the subject».
[134] § 8(a) of the Norwegian Personal Register Act granted individuals with a right to "block" the processing of data to prevent their use for the distribution of advertising materials or similar publications, which resembles existing "opt-out" mechanisms.

INSTITUTIONAL CONTROL – Institutional control mechanisms were subject to several adjustments aimed at an overall simplification of regulatory procedures. Easier notification mechanisms were preferred over licensing schemes[136], as they simply required controllers to declare the initiation of a processing activity, and a number of simplifications and exemptions were introduced when prior-authorizations of supervisory authorities were still required[137]. In parallel, data protection authorities[138] maintained and broadened their general oversight powers on data protection compliance and became an important ally and point of reference for individuals in the effective exercise of their rights[139].

CONSTITUTIONAL RECOGNITION - The rights-based approach that started to permeate this second phase of data protection evolution was reflected also in the inclusion of specific individual rights related to automated data processing in a number of national constitutions. The Austrian DSG was one prominent and peculiar example, being a statute in which ordinary norms alternated with constitutional provisions[140]. Among the latter, Article 1 was titled "Fundamental right to data protection" (*Grundrecht auf Datenschutz*), that was essentially connected to the protection of the right to respect for private and family life[141]. Portugal included specific rights concerning automated data processing in its 1976 Constitution, where Article 35 on the "Use of informatics" recognized to all citizens the right to access and correction to data related to them included in data banks[142]. After an intense debate, also Spain agreed to include Article

---

[135] Article 26 of the *Loi Informatique* introduced a «*droi de s'opposer a ce que des informationnes nominative la concernat fassent l'object dun treatment*». § 18 of the DSG included the consent of the data subject as one of the grounds to legitimise onward transmissions of data between private parties.

[136] In the *Loi Informatique*, prior consultation procedures were limited to public sector data processing, while Article 16 required private entities to send a "declaration". § 8 of the DSG also included a notification procedure before the initiation of a data processing. The BDSG included notification and registration obligations only for entities in the context of business data processing (§ 39). Pagano (n 103) 10–11; 27–28; 36.

[137] The *Loi Informatique* introduced a number of exemptions in Art. 17. The Norwegian Personal Register Act provided for a general prior authorization procedure ("King's consent") for all electronic registers or manual registers containing sensitive data and granted the King the power to exempt certain registers. ibid 66.

[138] For Germany, at federal level the Bundesbeauftragten für den Datenschutz, complemented with local Landesrecht zuständige Aufsichtsbehörde; in France the Commission Nationale Informatique et Libertés (CNIL); the Austrian Datenschutzcommission and the Norwegian Datatylsynet that complements the King's administrative powers.

[139] See e.g., § 14 of the DSG, Article 21 *Loi Informatique* and § 2 of the Norwegian Personal Register Act.

[140] Pagano (n 103) 9; González Fuster (n 59) 67.

[141] Specifically, §1(1) of the DGS stated: «Everyone has the right to confidentiality of personal data concerning him or her, insofar as he or she has an interest worthy of protection, in particular with regard to respect for his or her private and family life». See also González Fuster (n 59) 67–68.

[142] Further, Article 35 (2) prohibited the automated processing of sensitive categories of information (e.g., political convictions, religious beliefs or "private life") except if the data were in non-identifiable form; while

18(4) in its 1978 Constitution, which affirmed that the law had to limit the use of computers to ensure citizen's honour, personal and family intimacy ("*intimidad personal y familiar"*), as well as the full exercise of their rights[143].

	Interests protected	Participatory control	Institutional control
German Federal Data Protection Act – BSG (1977)	- Interests of the persons concerned worthy of protection	- Data subjects' consent (processing ground) - Right to information/access - Right to correction - Right to block (suspected inaccuracy) - Right to erasure	- Supervision of the Federal Data Protection Commissioner and local data protection authorities - Reporting/registration obligations (business activities)
French *Loi Informatique* (1978)	- Personal identity, human rights, private life, public and individual liberties	- Data subjects' consent (for sensitive data) - Right to oppose - Right to information (duty to inform) - Right to access (+ rectification, supplement, update) - Right to know and contest automated decisions	- Prior-authorization by (for public sector operations) or notification to (for private sector operations) National Information Commission - Supervision by National Information Commission - Public data processing register
Austrian Data Protection Act - DSG (1978)	- Right to confidentiality - Right to private and family life	- Right to information/access - Right to rectification - Right to erasure	- Notification/registration procedures - Supervision by Data Protection Authority
Norwegian Personal Register Act (1978)	Not expressly provided	- Data subjects' consent (in the context of opinion and poll activities) - Right to information/access - Right to rectification, supplement, erasure (i.e., duty to rectify, supplement, erase) - Right to "block" processing	- Supervision by the Data Inspectorate - Licensing schemes

Article 35 (3) prohibited the use of national unique numbers for interconnection purposes. See Pagano (n 103) 71.

[143] Article 18(4) of the 1978 Spanish Constitution stipulated: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

		(for advertising purposes)	

Table 3. Data protection acts 1977-1978

3.3 The rise of informational self-determination (early 1980s – 1995)

BACKGROUND - The technological progresses of the 1980s took data gathering and processing powers to another level, incrementing organizations' appetite for information[144]. The decentralization process of information collection was enhanced by an increased data mobility. Network technology and telecommunications made it possible for computers to become interconnected and communicate with each other, making information transmissions effortless and fast[145]. These developments reinforced the perception that information flows and organizational patterns were spiralling complex, with a growing fear of loss of control over the circulation of personal information[146]. This ever-evolving technological context moved the discussion around data protection even further. The connection between data protection and the safeguard of individual rights and fundamental freedoms became tighter, particularly in relation to the right to private life (i.e., the EU version of the right to privacy)[147]. Concurrently, the idea that data protection was more than a negative liberty to exclude others; that individuals should be able to determine and control the circulation of their information started to gain momentum[148]. Two events, in particular, characterized this period and influenced, in their own way, the data protection history of the decade.

INTERNATIONAL INSTRUMENTS – The '80s opened with the elaboration of the first international instruments that dealt with the processing of individual information. Cooperation efforts between European and non-European countries resulted in the adoption of two international conventions: the 1980 OECD Guidelines ("Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" of the Organization for Economic Cooperation and Development) and Convention 108 ("Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data") adopted in 1981 by the Council of Europe. The acts are explored in detail under par. 4 *infra*. Suffice here to mention that these instruments played a pivotal role in fostering

[144] Bygrave (n 14) 99.
[145] Mayer-Schönberger (n 67) 230.
[146] Bygrave (n 14) 108.
[147] González Fuster (n 59) 82.
[148] Council of Europe (n 66). In particular Rodotà (17), Simitis (22) and more generally the exchange of thoughts on the "Aspects of control in data protection" where subjective control mechanisms, in the form of individuals rights, and the need of effectiveness were strongly advocated.

data protection discussions around the globe, and in Europe in particular. The achievement of a shared understanding of principles and basic rules in the field of data processing prompted the adoption of legal instruments in this area and encouraged the convergence existing national laws. Despite not being legally binding, the OECD Guidelines were an extremely influential instrument at global level[149], particularly in non-European countries (such as Japan, Australia and New Zeland)[150]. Whereas, Convention 108 set a milestone in the development of norms on the processing of personal data mainly in European countries[151], contributing to the adoption of the UK Data Protection Act[152] and the Finnish Personal Data Register Act[153], and fostering discussions on the enactment of data protection statutes both in Netherlands[154] and Belgium[155]. It also represented the first international instrument to expressly establish a "right to data protection".

INFORMATIONAL SELF-DETERMINATION - A second event that marked the data protection debate in the '80s was the *avant-garde* "census decision" of the German Federal Constitutional Court, issued in 1983[156]. The triggering episode was once again related to the proposal of a German law on population census. The growing public opposition to the bulk collection of citizens' data, fueled by fears of information misuse and mass surveillance, had raised severe doubts on the law's constitutionality[157], that as a result was brought before the Federal Constitutional Court (*Bundesverfassungsgericht*, "BVerfG"). Against the backdrop of the constitutional issue, the German Court adopted what is considered a seminal ruling in data protection case law in that it recognized for the first time a "right to informational self-determination"

[149] González Fuster (n 59) 80; Giovanni Buttarelli, *Banche Dati e Tutela Della Riservatezza: La Privacy Nella Società Dell'informazione: Commento Analitico Alle Leggi 31 Dicembre 1996, Nn. 675 e 676 in Materia Di Trattamento Dei Dati Personali e Alla Normativa Comunitaria Ed Internazionale* (Giuffrè 1997) 37; OECD, 'The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines', vol 176 (OECD 2011) OECD Digital Economy Papers 176 76–79.)

[150] Bygrave (n 14) 32.

[151] González Fuster (n 59) 92; Buttarelli (n 149) 27.

[152] UK Data Protection Act 1984.

[153] Henkilörekisterilaki 471/1987.

[154] After withdrawing a first bill in 1981, a new bill was submitted in 1985 with the purpose of amending the Dutch Constitution to incorporate a general right to respect of the *persoonlijke levenssfeerwas*. The bill was enacted in 1989 as the *Wet persoonsregistraties.* González Fuster (n 59) 93.

[155] After a ten-year long discussion following the ratification of Convention 108, and a number of bills submitted to the Parliament, Belgium adopted the *Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (Act on the Protection of Privacy in relation to the Processing of Personal Data) in 1992. Pagano (n 103) 13–14; González Fuster (n 59) 94.

[156] BVerfG, Urteil v. 15.12.1983 zum VZG 83 (1 BVerfGE 65), "Volkszählungs Urteil".

[157] Giovanni Sartor, 'Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz"' (1986) XII Informatica e diritto 95, 97–98.

(*Informationelle Selbsbestimmung*), understood as the «power of individuals to determine, in principle, the disclosure and use of their personal data»[158]. The Court anchored its reasoning on the constitutional protection of individual personality[159], whose existence was derived from the combined reading of two fundamental values of the German legal system, "human dignity" (enshrined in Article 1(1) of the German Constitution)[160] and "self-development" (set forth in Article 2(1) of the German Constitution)[161]. According to the Court, the right to personality (*Persönlichkeitsrecht*), which had already been affirmed by previous jurisprudence[162], encompassed a right to self-determination that empowered individuals to determine for themselves when and to what extent they wished to disclose matters relating to their personal life[163]. Since technological advances increased the chances to access and gain influence on individuals' actions[164] and could inhibit the freedom of individuals to plan and to decide freely, hence to self-determine freely in the society[165], the Court concluded that the right to self-determination required to be adapted to this new technological dimension. According to the Court, the modern understanding of this right presupposed «the protection of individuals against the unrestricted collection, storage, use and transfer of their personal data»[166]. More importantly, it recognized that in order to achieve the latter, individuals needed to be able to maintain a level of determination with regard to the circulation of information concerning them (i.e., "informational self-determination")[167]. The Court's ruling had an undeniable impact on the development of

[158] BVerfGE65, 1, C II, 1(a).
[159] Sartor (n 157) 102–103.
[160] Art 1(1) of the German Constitution (*Grundgesetz*) states: «Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority». Translation from Hondius (n 69) 7 and for the Swedish Data Act 46.
[161] Art. 2(1) of the German Constitution (*Grundgesetz*) states: «Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law». Translation from Basic Law for the Federal Republic of Germany.
[162] See for an extensive review of the German Federal Court's case law on the matter Vincenzo Roppo, 'I Diritti Della Personalità' in Guido Alpa and Mario Bessone (eds), *Banche dati, telematica e diritti della persona* (CEDAM 1984) 73 ff.; Giovanni Sartor, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (an Parliamentary Research Service 2020) 100 footnote 15.
[163] Rouvroy and Poullet (n 48) 52–54.
[164] According to the Court it was «technically possible, with the help of automated data processing to store indefinitely and retrieve at any time, in a matter of seconds and without regard to distance, specific information of an identified or identifiable person», that could be further «combined […] with other collections of data to assemble a partial or essentially complete personality profile». This expanded the possibilities for consultation and manipulation, which could affect the conduct of the individual. BVerfGE 65, 1, C II, 1(a).
[165] BVerfGE 65, 1, C II, 1(a), Rouvroy and Poullet (n 48) 55.
[166] BVerfGE 65, 1, C II, 1(a), Sartor (n 157) 102.
[167] ibid 106.

data protection laws in Germany[168], primarily, but its influence reached many other European states[169] thus providing solid legal argumentations for the introduction of mechanisms that endowed individuals with control and participation powers over their data[170].

Variously affected by the two events described above, European data protection acts adopted or amended between the '80s and the '90s emphasized the linkage between data protection and the safeguard of fundamental rights and further stressed the active and participatory role of data subjects, in the form of a more structured "bulk" of subjective rights. The UK Data Protection Act (1984)[171], the Finnish Personal Data Register Act (1987)[172], the 1990 amendment of the German *BDSG*[173] , and the Belgian Data Protection Act (1992)[174] fall into this category, as well as some sectorial norms drafted to regulate specific activities[175].

OBJECTIVES - Most of these acts grounded data protection on specific individual rights. The United Kingdom was the most significant exception[176], whereas the Finnish Person Register Act, the amended BDSG, and the Belgian Data Protection Act all included in their scope the protection of individuals' privacy, interests, and rights (*henkilön yksityisyyden sekä hänen etujensa ja oikeuksien*)[177], the right to personality (*Persönlichkeitsrecht*)[178] or private life/personal sphere (*vie privée / zijn persoonlijke levenssfeer*)[179].

MAIN PROVISIONS - The regulatory framework focused on more technical aspects of data processing was not abandoned. On the contrary, in most of these norms, data

[168] Bygrave (n 14) 118.
[169] Kosta (n 93) 102. According to Mayer-Schönberg, besides the late amendments of the German Federal Data Protection Act (1990), also the 1986 amendment of the Austrian data protection law, the amendment of the Norwegian Personal Register Act and some parts of the Finnish Data Protection Act can be included among the "third generation" acts, which are influenced by the German Court's decision. Mayer-Schönberger (n 67) 231.
[170] Kosta (n 93) quoting Simitis.
[171] UK Data Protection Act 1984.
[172] Henkilörekisterilaki 471/1987.
[173] *Bundesdatenschutzgesetz* (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954)
[174] Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 18 maart 1992.
[175] Mayer-Schönberger (n 67) 223.
[176] González Fuster (n 59) 149.
[177] Section 1 of the Finnish Person Register Act.
[178] § 1 of the 1990 BDSG.
[179] Article 2 of the Belgian Data Protection Act.

protection principles were more elaborate, confidentiality and security rules were strengthened and the number of requirements increased[180].

PARTICIPATORY CONTROL - Data subjects' rights mirrored, for the most part, subjective rights already provided by the second-generation acts, although strengthened and extended. Rights to information, access, erasure and correction were generally more detailed[181] and stringent (e.g., the right to information of the Belgian Data Protection Act required that individuals were "immediately informed" when subject to a data processing, rather than "upon request" or at "reasonable intervals")[182]. Consent became also a stable presence. The UK Data Protection Act contained five references to the data subject's consent, necessary in particular to authorize disclosure requests[183]. In the Finnish Person Register Act the data subject's consent was one of the main grounds to legitimize the recording of data in personal files[184], to further communicate personal data[185] , and to combine different data files[186]. Under Belgian law consent was required to process medical data[187] and as basis for specific processing activities (e.g., to publish home information or include data on advertising lists)[188]. Finally, the amended BDSG kept consent as one of the processing legal basis (like the previous version), but it further detailed its requirements[189] and extended its scope of application to additional use-cases[190].

INSITUTIONAL CONTROL – Notification obligations and supervision by data protection authorities remained central institutional control mechanisms. Somehow opposed to the

[180] E.g., Schedule 1 of the UK Data Protection Act that detailed "The data protection principles", including fairness and lawfulness, purpose limitation, accuracy, storage limitation and Schedule 2 that clarifies the interpretation of each principle; Chapters 2 ("Collecting and recording personal data") of the Finnish Person Register Act, additional rules on the use and communication of data were included in Chapter 5.
[181] E.g., see Sections 21-25, principle 7 of Schedule 1 of the UK Data Protection Act.
[182] Art. 4(1) of the Belgian Data Protection Act. Paul Schwartz and Joel R Reidenberg, 'Commissioned Study: Online Services and Data Protection and Privacy. Regulatory Response' (European Commission 1998) 66–67.
[183] Kosta (n 93) 69–72. In particular: (i) without consent data controllers could not disclose information that related to a third-party person (§ 21(4)); (ii) consent legitimised disclosure of data in the payroll context (§ 23(2)), when data were processed for domestic or household activities (Section 33(5) or even when disclosure was not allowed under the Act (§ 34/6)).
[184] Section 5 of the Finnish Person Register Act, according to which in the absence of the data subject's consent or permission from the supervisory authority, personal data could be recorded in a personal file only if the person had a substantive association with the controller (e.g., customer or service relationship).
[185] Sections 18(1) and 19 of the Finnish Person Register Act.
[186] Section 20 of the Finnish Person Register Act.
[187] Art. 7 of the Belgian Data Protection Act.
[188] Schwartz and Reidenberg (n 182) 87.
[189] § 4 of the BDSG
[190] For example, for the storage, modification or use of personal data for different purposes than those of collection, consent was required, § 14 of the BDSG.

simplification trend that was taking hold in data protection acts around Europe, the UK Data Protection Act included extensive and stringent registration requirements for data controllers and computer bureaus (see Section 5 Part II), that were complemented by obligations to update and renew on a yearly basis the original registration. Declaration requirements for "any automated processing operation" were provided also in the Belgian Data Protection Act (Art. 17). The broad scope of these provisions was downsized by the inclusion of exemptions for certain categories of data processing. The BDSG and the Finnish Persona Register Act did contain certain notification obligations that were, however, limited to specific situations.

	Interests protected	Participatory control	Institutional control
United Kingdom Data Protection Act (1984)	/	- Data subject's consent (disclosure purposes) - Right to access - Right to correction - Right to erasure	- Registration obligations - Supervision by the Data Protection Registrar
Finland Person Register Act (1987)	- Privacy - "Interests and rights"	- Data subject's consent (processing basis) - Right to "inspection", i.e., notification/information and access - Right to rectification and error	- Notification obligations (for specific data processing operations) - Supervision of Data Protection Ombudsman
German Federal Data Protection Act (1990)	- Right to personality	- Data subjects' consent (processing basis more detailed) - Right to notification/information - Right to correction - Right to block (suspected inaccuracy) - Right to delete	- Registration obligations (private entities carrying out specific business activities) - Supervision by Federal Commissioner for Data Protection and state supervisory authorities
Belgian Data Protection Act (1992)	- Private life /private sphere	- Data subjects' consent (medical data) + opt-in rule in sectorial legislation	- Declaration requirements (with exceptions) - Supervision by the

		- Right to information - Right to access - Right to rectification	Commission de la protection de la vie privée

Table 4. Data protection acts 1980-1995

4 International framework

Since the 1960's the international efforts to investigate automated data processing and develop unified principles in the area intensified. Many international organization and non-governmental entities[191] started to foster cooperation and discussions on these topics.

The progressive adoption of national data protection acts across Europe urged the need to reach international consensus on key regulatory elements, to ensure harmonization and compatibility among national laws[192]. Specific concerns were in fact raised about the possibility that unintended divergences between domestic policy choices could create adverse effects on the free flow of personal data between countries, hindering social and economic development[193]. Equally, there was a fear of "data protectionism", that would lead states to develop legislations in the name of privacy protection, but with different national purposes in mind (e.g., protection of local technologies or home industries)[194].

International discussions resulted in the parallel development and almost concomitant adoption of two cardinal international instruments: the OECD Guidelines in 1980, and Convention 108 of the Council of Europe in 1981. As mentioned in paragraph 2.3, these instruments had a significant impact on the development of data protection legislations in Europe and around the world. The objectives of the 1980 OECD Guidelines and Convention 108 were similar: strengthen the protection of individuals (in particular their right to private life/privacy) and ensure the free flow of personal data across national

[191] Michael D Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (1980) 16 Stanford Journal of International Law 27, 45; Hondius (n 69) 75–77. Beside the OECD and the Council of Europe, the Nordic Council and other non-governmental organizations such as the International Federation for Information Processing (I.F.I.P.), the European Cooperation in Informatics (ECI) and the Intergovernmental Council of Automated Data Processing (I.C.A.) devoted attention to problems of data processing. Also, within the United Nations, the General Assembly adopted a resolution in December 1968 inviting the Secretary-General to undertake a study of human rights problems in connection with the development of science and technology.
[192] Council of Europe (n 66) 324; Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 40.
[193] OECD (n 149) 10; Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 28.
[194] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 28; Buttarelli (n 149) 37.

borders. The rights-based approach of Convention 108 versus the market-oriented background of the 1980 OECD Guidelines determined the different prominence and rationale behind the two instruments.

The following paragraphs explore the role of individual control over personal data in the context of these two international instruments.

4.1 The OECD Guidelines (1980)

The Organization of Economic Cooperation and Development ("OECD") is an intergovernmental organization established in 1961[195] with the mission to stimulate economic growth and promote the global economy and the expansion of world trade[196]. The original group of twenty founding members[197] was enlarged reaching the number of twenty-four during the '80s (when the 1980 Guidelines were adopted) and counts today thirty-seven countries worldwide[198].

4.1.1 Early activities of the OECD in the field of data processing

Concerns about the economic and social implications of computer developments were expressed in the OECD as early as the late '60s, increasing the international pressure to investigate issues relating to information processing and computerization[199]. Since 1968 multiple committees[200] were created, seminars[201] and studies[202] undertook to

[195] Originally founded as the Organization for European Economic Co-operation (OEEC), formed to administer American and Canadian aids under the Marshall Plan for the reconstruction of Europe after World War II, in 1960 a Convention was signed to transform the OEEC into the current OECD. The Convention entered into force in 1961.

[196] Article 1 of the Convention states that the aims of the OECD shall be to promote policies designed:«(a) to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy; (b) to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and (c) to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations».

[197] The OECD founding countries are: Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. Although the Netherlands, Luxembourg and Italy ratified the Convention one year after the other countries (in 1962), they are still considered to be part of the founding group.

[198] The list of current member countries can be accessed at http://www.oecd.org/about/members-and-partners/.

[199] González Fuster (n 59) 76; Bennett (n 101) 136.

[200] In 1968, the OECD Committee on Science Policy promoted the launch of a "*Computer Utilisation Programme*", and the setting up of a "*Computer Utilisation Group*" to study the the topic of "computer utilization" in depth (Hondius (n 69) 57.). The task of this group was to study the technological, economic and legal questions relating to computers and telecommunications. Bennett (n 101) 136. In 1972, the OECD created a *Data Bank Panel* to reflect on policy problems related to data processing in automated databases. González Fuster (n 59) 76.

[201] In March 1968, a ministerial meeting on Science of OECD Countries was devoted to the issue of "Gaps in Technology" González Fuster (n 59) 77. In 1974, an OECD Seminar on "Policy Issues in data protection and privacy" with data protection experts from both sides of the Atlantic was organized (OECD, "Policy issues in data protection and privacy. Concepts and perspectives. Proceedings of the OECD

discuss the technological and economic implications of computing and automated data processing.

As the '60s unfolded, the OECD started to consider the growing economic value of data and the importance to ensure an open circulation of information. Discrepancies among national approaches on international data transfers and the introduction of restrictions to data exports triggered concerns over the possibility that national provisions could create barriers to data flows[203], therefore hindering world trade and growth[204]. Transborder data flows became a top priority in the OECD agenda. Following the 1977 Symposium on "Transborder Data Flows and the Protection of Privacy", the OECD created a new Expert Group[205] that was entrusted in particular with the task of developing guidelines on basic rules governing transborder flow and the protection of personal data and privacy to facilitate a harmonization of national legislation[206]. In drafting the guidelines, the Expert Group was asked to work in strict collaboration with the Council of Europe, which at the time was working in parallel on "Convention 108" (see *infra* par. 4.2)[207]. The objective was to derive the fundamental processing principles emerging in those contexts and include them in a single intercontinental instrument so that they could become a worldwide benchmark, applicable to other members of the OECD[208], and

seminar 24th to 26th June 1974", OECD Informatics Studies, 10, 1976, Paris). The Seminar was followed in 1977 by a Symposium on "Transborder Data Flows and the Protection of Privacy" in 1977 (OECD, "Transborder Data Flows and the Protection of Privacy", Information Computer Communications Policy, 1. Proceedings of a symposium held in Vienna, Austria, 22-23 September, 1977. Paris, OECD, 1979).

[202] The Computer Utilisation Group published multiple studies under the OECD Series of *Informatics Studies*, among which a report on *Digital information and the privacy problem*, in 1971. Hondius (n 69) 57–58; Bennett (n 101) 136; González Fuster (n 59) 77; OECD (n 149) 9.

[203] M Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 International Data Privacy Law 6, 3. Legislators feared that data could escape national regulation due to data handlers "offshoring" data processing, i.e. transferring data to countries with less stringent protection, so-called "data havens". Bennett (n 101) 130; González Fuster (n 59) 77.

[204] Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (n 203) 8.

[205] The Expert Group on trans-border data flows and the protection of privacy, formally established in February 1978 by the Committee for Scientific and Technological Policy, which replaced the previous Data Bank Group. The Expert Group was chaired by Michael Kirby, Chairman of the Australian Law Reform Commission. Among the other experts of the Group also Mr. Freese (first head of the Swedish Data Protection Authority), Prof. Simitis (Data Protection Commissioner of the German federal state of Hesse) and Prof. Rodotà (later a member of the Italian Data Protection Authority and long-time advocate of privacy protection). Michael D Kirby, 'The OECD Privacy Guidelines @ 30. Remarks to the OECD Working Party for Information Security and Privacy' (Paris, 9 March 2010) 2; Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (n 203) 6–7.

[206] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 43.

[207] As well as to build on the previous works undertaken by the Nordic Council, the Council of Europe, the European Economic Community and academic writings. Explanatory Memorandum, paragraph 19; Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (n 203) 6.

[208] ibid.

reduce the fragmented framework of national barriers on the free flow of information[209]. The negotiations leading to the elaboration of the OECD Guidelines were arduous, primarily due to the contrasting approaches to information flows that ranged from economic-oriented positions to individual rights-based perspectives[210]. Finally, a compromised solution was achieved. In 1980, the OECD Council formally adopted a Recommendation concerning "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[211]. The Guidelines were formulated as an Annex to the Recommendation and did not have legally binding nature[212].

4.1.2 The OECD Guidelines 1980

OBJECTIVES - The OECD Guidelines had general character and reflected the policy choices embraced by Member countries over the years[213]. Within the overarching goal of harmonize national provisions, the Guidelines had two key objectives.

The first objective concerned achieving acceptance of minimum standards of protection of «privacy and individual liberties» in the processing of personal data[214]. Taking up the trend emerged in national data protection laws around Europe, the OECD Guidelines grounded data processing rules on (*inter alia*) the protection of individual fundamental rights. However, given the persisting national divergences as to which fundamental right was to be taken as grounding basis for data protection rules, the OECD adopted a cautious approach, in that the term "privacy" was swiftly followed with a generic reference to other "individual liberties"[215]. "Data protection" remained a fuzzy concept

[209] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 28.
[210] Generally, US positions clashed with European ones, which were more inclined to emphasize the dangers posed to individual rights. González Fuster (n 59) 77–78; Kirby, 'The OECD Privacy Guidelines @ 30. Remarks to the OECD Working Party for Information Security and Privacy' (n 205) 6–7.)
[211] Organisation for the Economic Cooperation and Development, "Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data", (23 September 1980).
[212] Even though some Member countries had emphasized the advantages of a binding international Convention with a broad coverage, it was eventually chosen to adopt a non-binding instrument, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises. Explanatory memorandum, par. 30. Kirby, 'The OECD Privacy Guidelines @ 30. Remarks to the OECD Working Party for Information Security and Privacy' (n 205) 8.
[213] Council of Europe (n 66) 324.
[214] Paragraph 1, Explanatory memorandum.
[215] González Fuster (n 59) 79. According to Kirby, the OECD Guidelines reflected the influence of the language and presentation of the US Privacy Study Protection Commission rather than that of the Council of Europe resolutions. Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 46.

and was rarely mentioned in the Explanatory Memorandum[216]. However, the Guidelines did admit that there was «a tendency to broaden the traditional concept of privacy and to identify a more complex synthesis of interests that can perhaps more correctly be termed privacy and individual liberties»[217], recognizing the expanding notion of the term. Individuals and their protection acquired a leading role also in the international data protection framework. The second objective, and possibly main driver of the Guidelines, was the safeguard of the free circulation of information, to avoid undue interferences and restrictions of transborder data flows that could obstruct the global economic and social growth[218].

MAIN PROVISIONS - From a structural perspective, the Guidelines were divided into five parts, which, besides some general definitions and specifications on the Guidelines' scope[219], included recommendations to ensure the free circulation of information among Members and prevent the establishment of artificial barriers to data flows, unless legitimate, as well as some mutual assistance and cooperation requirements[220].

The most relevant section of the Guidelines was Part Two, which laid down eight "basic rules"[221], in the form of principles on the processing of personal data, that Member countries were recommended to implement as minimum standards to protect privacy[222]. While some of these principles presented only the basic requirements for the collection and processing of data (e.g., data quality[223], purpose specification[224], security

[216] Paragraph 4 of the Explanatory Memorandum acknowledged that «it is common practice in continental Europe to talk about "data laws" or "data protection laws" (*lois sur la protection des données*), whereas in English speaking countries they are usually known as "privacy protection laws"».
[217] Paragraph 2, Explanatory Memorandum.
[218] Paragraph 25, let. c) and d) Explanatory Memorandum. See González Fuster (n 59) 80.
[219] The Guidelines applied to (i) manual and automated data processing; (ii) in both the private or public sector, provided the processing manner, context or data nature posed dangers to privacy and individual liberties. Paragraph (2)(a); Explanatory memorandum, para. 34-35, 43.
[220] Parts Three, Four and Five of the OECD Guidelines. Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 44.
[221] ibid 29 and 44.
[222] Buttarelli (n 149) 37; Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 27–29.
[223] Paragraph 8 of the OECD Guidelines on "Data Quality" stated that «Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date».
[224] The "Purpose Specification Principle" in Paragraph 9 of the OECD Guidelines clarified that it had to be possible to identify the purposes for which data were to be processed, not later than at the time of data collection, and that changes of purposes had likewise to be specified.

safeguards[225], accountability[226]) others, instead, referred to specific individual rights that Member countries were recommended to grant at national level to data subjects.

PARTICIPATORY CONTROL – Despite their market-oriented attitude, the OECD Guidelines stand out for a substantial number of principles that clearly envisaged an active and participatory role of individuals in the management of their personal data. More specifically:

- **Collection Limitation -** The Collection Limitation principle included in Paragraph 7 provided that «there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the *knowledge or consent* of the data subject». On the one hand, the principle encouraged policy makers to introduce limitations to data processing to prevent indiscriminate data collection and prescribed the ways (*lawful and fair means*) in which data should be collected to avoid deceiving or obscure collection practices[227]. More importantly, the Principle asserted that, depending on the circumstances, the "knowledge or consent" of the individual became prerequisites to data processing[228]. The awareness of the data subject, as a minimum standard, and his authorization were therefore necessary conditions for a lawful data processing[229].
- **Use Limitation -** The principle of Use Limitation enshrined in Paragraph 10 affirmed that: «Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the *consent of the data subject*; or b) by the authority of law». This principle acted in strict relation with the purpose specification principle (Paragraph 9). The latter required data to be processed only for the specific purposes disclosed at the moment of collection. The former, building up on the previous one, regulated cases of "further processing" for purposes different from the ones initially disclosed. Here again, the data subject's authorization was one of the two conditions that could derogate to the general prohibition to deviate from the original purpose[230].

[225] The "Security Safeguards Principle" under Paragraph 11 of the OECD Guidelines had a broad scope as it required the implementation of «reasonable security safeguards» against risks of loss or unauthorized access, destruction, use, modification or disclosure of data.
[226] The "Accountability Principle" provided that a data controller should be accountable for complying with measures which give effect to the principles stated above.
[227] Explanatory Memorandum, paragraph 52.
[228] Kosta (n 93) 32.
[229] Explanatory Memorandum, paragraph 50.
[230] Explanatory Memorandum, paragraph 55; see Kosta (n 93) 33.

- **Openness –** Paragraph 12 was formulated in relatively high-level terms providing that «there should be a general policy of openness about developments, practices and policies with respect to personal data. *Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller*». The principle was considered a prerequisite for the "Individual Participation Principle" (see *infra*) to be effective[231]. Basically, it imposed a transparency obligation on data controllers in relation to their processing activities. In practice, this meant that individuals had to be able to obtain information about data processing concerning them without unreasonable efforts or costs[232]. There was no restriction on the ways in which transparency could be achieved and it was not necessarily addressed only the concerned data subjects. Openness could be realized by «regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies»[233], which entailed a broad understanding of transparency and collective control.
- **Individual Participation –** The principle of Individual Participation (Paragraph 13) was a peculiarity of the OECD Guidelines and it was generally regarded as one of the most critical privacy safeguards[234]. Rarely, in fact, data protection acts contain this principle in such explicit terms[235]. As already noticed for the national laws explored above, concept of "individual participation" and "individual control" manifested more obliquely as a set of different rules that empower individuals by introducing certain subjective rights[236]. The OECD Guidelines, on the contrary, were the only instrument in which this principle was expressed in clear terms. The principle stipulated that data subjects should have three primary rights: (a) to access, in terms of having confirmation of whether data concerning them were processed, and to obtain those data in a timely and reasonable manner[237]; (b) to reason, namely to obtain an explanation if the latter requests for information were

[231] Explanatory Memorandum paragraph 57.
[232] Explanatory Memorandum, paragraph 57.
[233] Ibid.
[234] Explanatory Memorandum, paragraph 58.
[235] Bygrave (n 14) 64.
[236] ibid.
[237] Par. 13(a) and (b) of the OECD Guidelines; Explanatory Memorandum, paragraph 59.

rejected[238]; and (c) to challenge data processing relating to them in a broad sense (i.e. data controllers, before courts, administrative bodies and professional organs) and if successful to have the data erased, rectified, completed or amended[239].

INSTITUTIONAL CONTROL – Considering their nature, the OECD Guidelines did not explicitly call for the establishment of institutional control mechanisms to ensure compliance with the principles set forth in the Guidelines. Par. 19(d) of the Guidelines simply recommended that Member countries should endeavour to «provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles»[240].

4.1.3 In the aftermath of the 1980 OECD Guidelines

In the years following the adoption of the 1980 Guidelines, the OECD promulgated further declarations and recommendations concerning data flows and privacy, to express its interest and restate its commitment on the subject matter[241].

Thanks to their technology-neutral approach, their simple conceptual language and the recognition of different domestic legal cultures, the 1980 OECD Guidelines were able to remain relevant and survive a number of societal and technological changes for a number of decades[242].

However, in 2013, the OECD finally decided to revise its 1980 Guidelines for the first time since their launch[243]. Despite the substantial and comprehensive updating work, no major innovations were introduced with regard to the principle of "Individual Participation" and the multiple subjective rights already included in the 1980 version. More space was instead provided to monitoring and enforcement mechanisms, in that

[238] Par. 13(c) of the OECD Guidelines; Explanatory Memorandum, paragraph 60.
[239] Par. 13(d) of the OECD Guidelines; Explanatory Memorandum, paragraph 61.
[240] According to the Explanatory Memorandum, paragraph 19(d) permitted different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise.
[241] In 1985, a "Declaration on Transborder Data Flows" OECD, "Declaration on Transborder Data Flows", (available at http://www.oecd.org/internet/ieconomy/declarationontransborderdataflows.htm) was issued, followed in 1998 by a "Declaration on the Protection of Privacy in Global Networks" (available at http://www.oecd.org/sti/ieconomy/1840065.pdf) both reaffirming the OECD commitment to protect free information exchange and privacy. González Fuster (n 59) 80.
[242] Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (n 203) 9–11.
[243] The OECD 2013 "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" are available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf .

the Guidelines now make it explicit the need to establish and maintain "privacy enforcement authorities"[244].

	Interests protected	Participatory control	Institutional control
OECD Guidelines 1980	- Privacy and other individual liberties - Free flow of personal data → free market and trade	- Data subject's consent to data processing (under the Use Limitation and Openness Principles) - Right to access - Right to reason - Right to challenge (all under the Individual Participation Principle)	(Left to Member countries to decide)

Table 5. 1980 OECD Guidelines

4.2 Convention 108 (1981)

The Council of Europe ("CoE") is an international organization established in 1949[245], whose membership, originally including ten European countries[246], increased to twenty-two by the mid '80s and counts now forty-seven states[247]. The aim of the CoE is to achieve a greater unity between its members for the purpose of (i) safeguarding and realizing common ideals and principles and (ii) facilitating their economic and social progress[248]. The protection and realization of human rights and fundamental freedoms have been a corner stone of the CoE's agenda, to the extent that in 1950 the CoE adopted its own catalogue of human rights[249], the European Convention on Human Rights (ECHR).

[244] A new provision in Part Five ("National Implementation") calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an "objective, impartial and consistent basis" [paragraph 19(c)].
[245] Treaty n. 001 on the Statute of the Council of Europe, 5 May 1949, which entered into force on 3 August 1949. For a short overview of the CoE origins and foundations: https://www.coe.int/en/web/yerevan/the-coe/about-coe/overview.
[246] The founding members of the CoE were Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the United Kingdom.
[247] All twenty-seven members of the European Union are part of the CoE, in addition to other twenty European states. Further, six countries (Canada, Holy See, Israel, Japan and United States) have been granted "observer" status. The list of CoE current Member countries and observers can be consulted here: https://www.coe.int/en/web/tbilisi/the-coe/objectives-and-missions Last visited on 9 July 2021.
[248] Art. 1(a) of the Statute states: «The aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage and facilitating their economic and social progress».
[249] González Fuster (n 59) 81.

4.2.1 Early activities of the CoE in the field of data processing

The engagement of the CoE in the field of data protection stemmed from the conclusion that Article 8 of the ECHR[250] and domestic laws had a series of shortcomings in light of new technological developments. Following two reports of the CoE Legal Committee, which reviewed the dangers to individual's rights inherent in technological developments and argued that particular attention should be paid to violations of the right to privacy[251], the Parliamentary Assembly of the CoE adopted Recommendation 509 (1968) on Human Rights and modern Scientific and Technological Developments[252]. The Recommendation declared that «*newly developed techniques*»[253] represented «a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the ECHR»[254] and it advised further studies on the subject[255]. The recommendation was followed in 1970 by an interim report that, updating previous anticipations, pointed out a new area of concern for the right to privacy: the use of computers[256]. As a result, in 1971 a Committee of Experts was established to specifically investigate the protection of privacy with respect to computers, and in particular the creation of electronic data banks[257]. At the same time, growing discussions at national level on the adoption of local norms on data processing and computer usage urged a joint action[258].

[250] Art. 8 (1) ECHR enshrines the "Right to respect for private and family life, home and correspondence". Despite some initial disagreements, this right was eventually considered the EU translation of the Anglo-Saxon based right to privacy. According to Gonzales, the preference for the term "private life" could presumably be explained by taking into account the influence of the French word "vie privèe". Since the adoption of the ECHR, no European institution, not even the European Court of Human Rights, appeared to have used the word "privacy" in reference to the content of Article 8 ECHR, up until 1967-1968 when the first analysis on the protection of human rights and technological developments were carried out. From that moment, the word privacy was more freely associated to the interests safeguarded by Article 8 ECHR. ibid 82–84.

[251] Committee on Legal Affairs and Human Rights, 1968.

[252] Council of Europe, "Recommendation 509 (1968) on Human Rights and modern Scientific and Technological Developments", adopted by the Assembly on 31st January 1968 (16th Sitting).

[253] The modern technologies referred to in the Recommendation concerned in particular «phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda». Recommendation 509 (1968) paragraph 3.

[254] ibid.

[255] Recommendation 509 (1968), paragraph 8(1).

[256] González Fuster (n 59) 84. The findings of the interim report included also the conclusion that the ECHR framework was not sufficient to offer protection, because it did not extend to private entities and was only applicable to interferences by public authorities. Hondius (n 69) 65; Bennett (n 101) 133–134.

[257] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 40; Hondius (n 69) 66.

[258] González Fuster (n 59) 85; Hondius (n 69) 66.

4.2.2 Resolution 73 (22) and Resolution 74 (29)

The works of the Expert Committee took the shape of two seminal resolutions[259] containing basic principles on automated data processing[260].

RESOLUTION 73(22) - The first, adopted in 1973, was Resolution 73(22) on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector[261]. Resolution 73 22) annexed ten general principles and called upon CoE Member States to take all the necessary steps to give effect to these principles in their national legislations. "Privacy" was mentioned in the very title of the Resolution, however no further explanation was provided to define or delimit the notion[262]. Also "intimate private life" was mentioned among the provisions of the Resolution[263], as well as "unfair discrimination" as one of the criteria that had to limit data collection and processing. The principles of Resolution (73)22 referred mainly to general criteria that the collection, processing and storage of information needed to be subject to, in particular in terms of: quality of the information ("accurate and up to date")[264]; appropriateness and limited purposes[265]; fair means of collection[266]; defined storage periods[267]; correction and erasure obligations[268]; data security and authorized access to information[269]; and statistical data[270].

PARTICIPATORY CONTROL - Only Principle 6 of the Resolution expressly provided for an individual right of the persons concerned by the processing, namely «the *right to know* the information stored about him, the purpose for which it has been recorded, and

[259] Before 1979, recommendations adopted by the Committee of Ministers were issued in the "Resolutions" series of adopted texts. These are non-binding legal instruments. https://www.coe.int/en/web/cm/adopted-texts-information#Resolutions .
[260] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 40; Hondius (n 69) 66..
[261] Committee of Ministers of the Council of Europe, "Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector", 26 September 1973 (224th meeting of the Ministers' Deputies).
[262]González Fuster (n 59) 85.
[263] Principle 1 of Resolution (73)22 states: «In general, information relating to the *intimate private life* of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated».
[264] Principle 1 of Resolution (73)22.
[265] Principles 2 and 5 of Resolution (73)22
[266] Principle 3 of Resolution (73)22.
[267] Principle 4 of Resolution (73)22.
[268] Principle 7 of Resolution (73)22.
[269] Principle 8 and 9 of Resolution (73)22.
[270] Principle 10 of Resolution (73)22.

particulars of each release of this information». The provisions of Resolution 73 (22) include some of the central elements later incorporated into Convention 108[271].

RESOLUTION 74(29) - A second resolution was adopted by the CoE a year after the first one, this time addressing data processing in the public sector, namely Resolution 74(29) on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector[272]. Along the lines of Resolution 73(22), the second resolution took the form of recommendations for Member States to put into effect the eight principles laid down in the resolution in their jurisdictions. The principles are very similar to the ones provided for the private sector. The guiding idea was fundamentally that the same rules should apply to both spheres[273]. The second resolution, like the first one, addressed the quality, accuracy and security of data; appropriateness and limitation of purposes; as well as adequate storage periods[274].

PARTICIPATORY CONTROL – Nothing much was added in Resolution 74(29) compared to the previous one. The right of individuals «*to know information stored about him*»[275] was restated and a general transparency duty based on which «*the public*» had to «be kept regularly informed about the establishment, operation and development of electronic data banks in the public sector»[276] was included.

	Interests protected	Participatory control	Institutional control
Resolution (73)22	- Privacy / intimate private life of individuals - Non-discrimination (?)	- Right to information/access	/
Resolution (74)29	- Privacy / intimate private life of individuals - Non-discrimination (?)	- Right to information/access (+right of the public to be informed of the creation of public data banks)	/

Table 6. CoE Resolutions 1973-1974

[271] Buttarelli (n 149) 4.
[272] Committee of ministers of the Council of Europe, "Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector", 20 September 1974 (236th meeting of the Ministers' Deputies).
[273] Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 40.
[274] Respectively, Principles 2, 3 and 4 of Resolution 74(29).
[275] Principle 5 of Resolution 74(29).
[276] Principle 1 of Resolution 74(29).

4.2.3 CoE Convention 108

In the years following the adoption of the two Resolutions, the CoE monitored their implementation and reviewed the state of advancement of national legislation in the area. The growing number of data protection laws in European countries and the emergence of relevant disparities called for a renewed joint effort and a more robust international instrument[277]. In 1976 a new Committee of Experts was formed with the task to draft a Convention on the protection of privacy in relation to data processing[278]. The work of the Committee[279] was carried out in close cooperation with the OECD, to ensure international alignment on the free flow of information principle, and with the European Community Institutions[280]. Finally, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (commonly known as "Convention 108")[281] was adopted by the Committee of Ministers on September 1980 and opened for signatures in 1981. Contrary to the previous Resolutions and to the 1980 OECD Guidelines, Convention 108 was a legally binding instrument on the signatory parties, but had not self-executing character.

OBJECTIVES - Although the free flow of data was mentioned among the purposes of Convention 108, the main aim of the Convention was to secure for every individual the «respect for *his rights and fundamental freedoms*, and in particular his *right to privacy*, with regard to automatic processing of personal data relating to him», which was altogether was defined "data protection"[282]. This was the first time that an international instrument explicitly recognized and defined the notion of "data protection"[283]. The concept still lacked autonomous status, as it was conceived as instrumentally

[277] Buttarelli (n 149) 8–9; Kirby, 'Transborder Data Flows and the Basic Rules of Data Privacy' (n 191) 41.
[278] González Fuster (n 59) 86.
[279] The Committee of Experts on Data Protection, initially placed under the authority of the European Committee on Legal Co-operation (CDCJ), was later renamed Project Group on Data Protection (CJ-PD). Explanatory Report of Convention 108, paragraph 1 and 17. See also ibid 86–87; Buttarelli (n 149) 6.
[280] In February 1980, the Parliamentary Assembly of the CoE adopted a Resolution welcoming European Parliament's interest, and inviting it «to direct its attention to how action within the framework of the European Communities could most effectively strengthen the principles and provisions to be embodied in the convention on data protection of the Council of Europe» as well as to call on national parliaments to press for the introduction of legislation on data protection.
[281] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.
[282] Article 1 of Convention 108.
[283] The only previous reference was contained in German law ("*Datenschutz*"), although it was never clear what the term ought to identify.

connected to the safeguard of other rights and freedoms, especially the right to privacy[284].

MAIN PROVISIONS - From a structural perspective, Convention 108 consisted of five chapters, whose provisions were aligned with the OECD positions of avoiding obstacles to the free flow of information except for some limited derogations and encouraging mutual assistance and cooperation. Similar to the OECD Guidelines, the most valuable chapter, for the purposes of this work, is Chapter II that listed the "Basic principles for data protection" that Members were expected to implement in their domestic laws[285]. The principles established only a standard floor of protection and did not affected the possibility for the Parties to introduce additional and broader measures of protection[286]. Most of these general provisions placed particular emphasis on "data" rather than "individuals"[287], as they included data quality recommendations (adequacy, relevance, accuracy) and requirements for their collection and storage (fairly and lawfully, for specified and legitimate purposes, for limited time)[288]. Specific provisions were devoted to the limitations to the processing of "special categories of data"[289] and data security[290].

PARTICIPATORY CONTROL - The only article that shifted the focus from the data/processing to the individual was Article 8 titled "Additional safeguards for the data subject". The Article listed a series of "safeguards" that Parties to the Convention were encouraged to include as domestic rights in their legal system. No mention was made to

[284] González Fuster (n 59) 88–89. Explanatory memorandum (1): «The object of this convention is to strengthen data protection, i.e., the legal protection of individuals with regard to automatic processing of personal information relating to them».

[285] See Article 4 of Convention 108. The measures employed to translate these principles into national legislations were up to the Parties to decide. They could take different forms, depending on the legal and constitutional system of the State concerned: apart from laws they could be regulations or administrative guidelines. Explanatory Report, paragraph 39.

[286] Like Art. 60 of the ECHR, also Convention 108 included a norm on the extension of protection by which «none of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention» (Article 11). See Buttarelli (n 149) 20.

[287] The legislative technique used by the CoE was criticized by some scholars due to its alleged focus on "data" rather than "individuals", resuming the technology-oriented outlook of the first-generation laws. Instead of creating a framework of individual rights, related safeguards and limits, the Convention mainly provided for criteria connected to the quality and security of the data. ibid 10 see footnote 28.

[288] Article 5 of Convention 108.

[289] Article 6 of Convention 108 provided that: «Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions». The list was not meant to be exhaustive, since contracting States could further expand the categories of sensitive data. See paragraphs 43-48 of the Explanatory Report.

[290] Article 7 of Convention 108 was drafted in very general terms, requiring that «appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination».

a general right or principle of data subjects to "participate" to the data governance or to maintain a "control over their data". The safeguards mentioned by Article 8 translated into the following subjective rights:

- **Right to information** – This included a right to know the existence of automated personal data files, its primary purposes and on the identity of the controller of the files[291];
- **Right to access** – This provided a right to have confirmation, without undue delay or costs, of whether personal data relating to him were stored in the automated data file and to obtain them in an intelligible form[292];
- **Right to rectify or erasure** – The right included the possibility to obtain the rectification or erasure of data if processed unlawfully[293];
- **Right to have a remedy** – This was limited to the cases in which one of the requests above mentioned were not fulfilled[294].

4.2.4 In the aftermath of Convention 108

The activities of the CoE on data protection did not slow down with the adoption of Convention 108 and continued in the following years with a considerable number of acts that translated and adapted the Convention's principles in specific sectors[295]. By way of example, *ad hoc* recommendations were issued with regard to data processing in automated medical banks[296]; in the context of scientific research and statistics[297]; for direct marketing purposes[298] and for social security purposes[299].

Following a review process started in 2011, with the objective to update Convention 108 in light of the challenges raised by new information and communication technologies, in 2018 a modernised version of Convention 108[300] ("Convention 108+") was approved.

[291] Article 8 (a) of Convention 108. The wording of this letter took into account the variety of rules of domestic law giving effect to this principle, e.g., via a list included in a public index or, where no such publicity rule applied, via a communication to a person at his request. Explanatory Report, paragraph 51.
[292] Article 8 (b) of Convention 108; Explanatory Report, paragraph 50, 52.
[293] Article 8 (c) of Convention 108; Explanatory Report, paragraph 50, 52.
[294] Article 8 (d) of Convention 108; Explanatory Report, paragraph 50.
[295] Buttarelli (n 149) 29–36.
[296] Recommendation (81) 1 on regulations for automated medical data banks, adopted on 23 January 1981. See Camera dei deputati, *Banche Dati e Tutela Della Persona* (1981) 521.
[297] Recommendation (83) 10 on the protection of personal data used of scientific research and statistics, adopted on 23 September 1983. See *Dir. Informatica* 1985, (369)
[298] Recommendation (85) 20 on the protection of personal data used for purposes of direct marketing, adopted on 1 October 1985. See *Dir. Informatica*, 1986 (992).
[299] Recommendation (86) 1 on the protection of personal data used for social security purposes, adopted on 23 January 1986.
[300] Adoption of Amending Protocol CETS No. 223 for the modernization of Convention 108.

Convention 108+ reaffirmed and strengthened its original principles, while laying down additional safeguards adjusted to the new technological reality[301]. In line with other international and regional trends (e.g., the 2013 OECD Guidelines, *supra*, and Regulation (UE) 2016/679, *infra*), Convention 108+ placed renewed emphasis on data subjects: the Preamble of the Convention expressly mentioned a «*person's right to control of his or her personal data and the processing of such data*»[302]. The free, informed specified and unambiguous consent became one of the two essential pre-requisites for a lawful data processing[303] and the catalogue of individual rights was further extended (including references to profiling and automated-decision making)[304]. Convention 108+ is currently awaiting to enter into force, upon ratification by all Parties to Convention 108, or in any case on October 2023.

	Interests protected	Participatory control	Institutional control
Convention 108	- Human rights and individual freedoms (in particular their right to privacy)	- Right to information - Right to access - Right to rectify and erase - Right to remedy	- Supervision by Data Protection Authority (under Protocol 2001)

Table 7. Convention 108

5 The European Union framework

Alongside national movements and international mobilization, also the European Community had started to pay attention to the data processing debate. Slowly, but consistently, a third "regional" dimension in the regulation of data processing emerged with the aim to achieve broader harmonization in the Community area.

After the first hesitant steps in the early 1970s, the route taken since then by the European Community, first, and European Union, after, has brought to light some of the most important pieces of legislation in the data protection realm. Directive 95/46/EC,

[301] For example, the Convention expressly includes new principles of privacy by design and accountability.
[302] Preamble of Convention 108+ states that: «it is necessary to *secure the human dignity and protection of the human rights and fundamental freedoms* of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, *personal autonomy* based on a person's right to control of his or her personal data and the processing of such data».
[303] Article 5(2) of Convention 108+.
[304] Article 9 of Convention 108+.

which crystalized the early efforts of the European Union to achieve better harmonization within its Member States, was later followed by the adoption in 2000 of the Charter of Fundamental Rights of the EU that marked a crucial moment in the recognition of a standard set of fundamental values across EU countries (including a "right to data protection") and by further legislative activity in some specific sectors (e.g., Directive 2002/58/EC). Finally, the adoption of Regulation 2016/679/EU lead to the most comprehensive reform that data protection has experienced so far.

This paragraph investigates the role of data subjects and their right to control in each of the above-mentioned acts.

5.1 Directive 95/46/EC: the "parent" Directive on the protection of personal data

5.1.1 Early activities of the EC

The European Community ("EC")[305] started to show some interest in the processing of information moved, on the one hand, by concerns on the growing US dominance in the market of computers, as a possible barrier to the economic development of the Community[306], and, on the other hand, by concerns on the weak protection of individual rights and freedoms of European citizens in view of new technological developments[307]. The existence of these two issues, the one dealing with the free flow of data to strengthen the Community single market, the other concerned with the limits of data processing to protect citizens, has characterized and shaped the debate on data protection in Europe[308]. Following the positions of previous international instruments, the EU action has also taken into account both aspects (free flow of data and data processing regulation), seeking a difficult balance between conflicting objectives, not without ambiguities[309]. The initial focus on market-driven objectives, due to the mainly economic purposes upon which the European Community had been built, has in time given way to a more pronounced rights-based approach to data protection, that

[305] Originally including the 1951 European Coal and Steel Community (ECSC), the 1957 European Economic Community (EEC) and the European Atomic Energy Community (Euratom), in 1992 the European Communities were merged under the Maastricht Treaty that formally established the "European Union". The six founders of the EC (Belgium, France, Italy, Luxembourg, the Netherlands, and West Germany) were soon joined by other states. The EU counted 15 countries in 1995 (at the time of the adoption of Directive 95/46/EC) and 28 in 2016 (at the time of the adoption of Regulation 2016/679(EU)).
[306] Hondius (n 69) 70–72; González Fuster (n 59) 111.
[307] Hondius (n 69) 71.
[308] Roberto Pardolesi and Alessandro Palmieri, 'Il Codice in Materia Di Protezione Dei Dati Personali e l'intangibilità Della "Privacy" Comunitaria' (2004) IV Foro italiano 59, 63.
[309] Francesco Macario, 'La Protezione Dei Dati Personali Nel Diritto Privato' in Vincenzo Cuffaro and Vincenzo Ricciuto (eds), *La disciplina del trattamento dei dati personali* (G Giappichelli 1997) 15 and 17.

received formal validation with the adoption of the Charter of Fundamental Rights of the European Union (see *infra* par. 5.2) and its constitutionalization under the Lisbon Treaty[310].

Since the 1970s', European Institutions adopted multiple documents to foster a broader debate on the data processing phenomenon and to encourage the European Parliament to take action[311]. When in 1981, Convention 108 was adopted, the European Commission warmly welcomed it as an adequate instrument to create a common playing field in Europe on data protection rules, and encouraged Members States to ratify it[312]. Taking a cautionary position, the Commission decided to assess the successful implementation of Convention 108 among its Members before starting to work on a binding legislative act of its own, as it considered the time not yet ripe for this course of action[313]. While, convention 108 had indeed been successful in drawing attention on the "data protection" topic[314], delays in its ratification and lack of consistency in national implementations constituted serious obstacles to the development of the internal market, where the processing of personal data was to play an increasingly important role[315]. The formal establishment of a European Union in

[310] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.
[311] See for example the EU Commission, "Communication to the Council, titled Community policy on data processing", 1973; Legal Affairs Committee of the European Parliament, "Interim Report drawn on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing", Working Documents 1974–1975, 1975; European Parliament "Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing", 1975; European Parliament "Resolution on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing", 1976; Data Processing and Individual Rights Sub-committee at the European Parliament, "Bayerl Report", E.P. Doc. 100/79, 1979; European Parliament "Resolution on the protection of the rights of the individual in the face of technical developments in data processing", 1979.
[312] European Commission, 'Commission Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (87AD) 81/679/EEC Par. 5.
[313] In its 1981 Recommendation, the European Commission reserved the «right to propose that the Council adopt an instrument on the basis of the EEC Treaty» if all the Member States did not sign and ratify Convention 108 within a reasonable time. Ibid.
[314] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' 20 <https://edps.europa.e/ite/d/ile/ublicatio/4-09-15_article_eui_en.pdf>; Fiona Carlin, 'The Data Protection Directive: The Introduction of Common Privacy Standards' (1996) 21 European Law Review 65, 65.
[315] European Commission, 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data' (1990) COM/90/314FINAL-SYN 287 3; Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 9.

1993[316] and the abolition of customs in 1995[317] further accelerated the need to deliver a functioning EU Single Market[318].

As a result, in 1990, the EC announced the adoption of a package of proposals, that included a proposed directive concerning the protection of individuals in relation to the processing of personal data[319]. After five years of intense negotiations[320], Directive 95/46/EC[321] ("DPD") was finally adopted.

Only a couple years later, the DPD was joined by Directive 97/66/EC[322], replaced soon after by Directive 2002/58/EC[323] (so called "e-privacy Directive"), that included sectorial norms aimed at particularize data protection rules in the specific area of electronic communication (including for example "cookie" rules). Contrary to the DPD, that has now been replaced by Regulation (EU) 2016/679 ("GDPR"), which modernizes the framework on data protection (analysed hereinafter), the 2002 e-privacy Directive remains fully applicable. The review works that should lead to the adoption of a new e-privacy Regulation are still, at the moment of writing, under way[324]. Hence, while the next paragraph focuses specifically on the (now repealed) provisions DPD, references to provisions of the e-privacy Directive, where relevant to our analysis, will be

[316] Treaty on European Union (Treaty of Maastricht) [1992] OJ C 191/01, which came into force in 1993.
[317] When the European single market formally entered into force, upon expiration of the final deadline set by the Single European Act [1987] OJ L 169/01. See also European Commission, 'Completing the Internal Market — White Paper from the Commission to the European Council' (1985) COM (85) 310 final.
[318] Franco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* (Seconda ristampa, G Giappichelli 2016) 64–65.)
[319] European Commission, 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data' (n 315).
[320] For a detailed analysis of the procedure and heated debates within EU institution, see González Fuster (n 59) 125–129; Buttarelli (n 149) 39–52.
[321] Directive 95/46/EC of the European Parliament and 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.
[322] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[323] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The e-Privacy Directive protects more generally "privacy in electronic communications", regardless of whether the information exchange concerns personal or non-personal data, and, in some instances, it offers protection also to legal entities and not only to "data subjects" as natural persons. However, when personal data processing operations are involved, the e-Privacy Directive operates as a *lex specialis* in respect to general data protection norms; hence e-Privacy rules prevail in regard to data processing in the context of electronic communications.
[324] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2017) COM(2017) 10 final.

incorporated under the paragraph analysing the GDPR, to complement the current and applicable legal framework on data protection.

5.1.2 Directive 95/46/EC

OBJECTIVES - The DPD was strongly guided by the principles and purposes set out in Convention 108[325], but the 1980 OECD Guidelines' influence was also visible.

The objective of the DPD, as mentioned above, was dual: (i) the protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data[326] and (ii) the prohibition of restrictions to personal data flows between Member States[327]. Despite the market-based orientation of the text, it was evident the centrality that the DPD conferred to individuals, not only in their quality of "consumers" but as fundamental rights-holders[328]. The linkage between the protection of personal data and the safeguard of individual rights and freedoms was evident already starting in the DPD recitals, where data protection was functionally related to the protection of other rights, in particular the right to privacy (differently translated as *vita privata, vite privèe, Privatsphäre*)[329]. Contrary to the OECD Guidelines, however, there was no reference in the DPD to a general principle of "individual participation" or "control" to the circulation of their information, nor a specific indication of other fundamental rights (e.g., informational self-determination) that embedded the idea of a more active and participatory role for individuals.

MAIN PROVISIONS - Conceptually, the DPD was divided into four main parts concerning: (i) general rules on the lawfulness of the processing of personal data (Chapter II); (ii) the transfer of personal data into third countries (Chapter IV); (iii) judicial remedies, supervisory authorities and the new Working Party on the protection of individuals (Chapter III and Chapter VI) and the community implementing measures (Chapter VII).

The body of basic rules in Chapter II included a range of principles and obligations that focused on data quality, security and confidentiality, which translated into specific

[325] See notably Recital 11 of Directive 95/46/EC that states that «the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data».
[326] Article 1(1) of the DPD.
[327] Article 1(2) of the DPD.
[328] Macario (n 309) 12.
[329] Recital 10 of the DPD.

requirements and conditions for the lawful processing of data[330]. The basic principles stipulated by Convention 108 and by most national traditions on data protection were reiterated and further supplemented. In particular, similarly to Convention 108, the DPD provided a general "data quality" principle that referred not only to the quality of data *strictu sensu*[331] («adequate, relevant and not excessive in relation to the purposes of processing»[332], accurate and up to date[333]), but also to the modalities of collection («collected for specified, explicit and legitimate purposes»[334]), processing (processed fairly and lawfully[335] and not further processed in incompatible ways) and storage (only as long as necessary for the purposes of the processing[336]). The DPD further established six legal grounds, whose presence legitimized the processing of personal data[337] (among which the "data subject's consent") and introduced special restrictions to the processing of "sensitive categories of data"[338], echoing related provisions contained in national data protection acts[339], as well as in Convention 108[340]. Specific confidentiality and security norms were laid down, particularly concerning the regulation of other entities involved in the processing of data[341] and the implementation of appropriate technical and organizational measures[342]. An entire chapter was devoted to rules governing data transfer to third countries, where the balancing between the dual interests protected by the Directive became more evident[343].

PARTICIPATORY CONTROL – Within this general framework, the DPD included specific provisions that granted data subjects with individual rights and decision-making powers to exercise a level of control on the use and circulation of their data. Since the DPD was essentially a synthesis between existing domestic legislations and

[330] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 9.
[331] Macario (n 309) 29; Pizzetti (n 318) 81.
[332] Article 6(1)(c) of the DPD.
[333] Article 6(1)(d) of the DPD.
[334] Article 6(1)(b) of the DPD.
[335] Article 6(1)(a) of the DPD.
[336] Article 6(1)(e) of the DPD.
[337] See Macario (n 309) 29–31.
[338] Art. 8 DPD established a general prohibition for the processing of these data, with some exceptions.
[339] See e.g., the prohibitions included in the French and Norwegian data protection acts.
[340] Pizzetti (n 318) 83.
[341] Article 17 (2-4) DPD; see further ibid 97.
[342] "Data processor", Article 17 (1) DPD; see further Macario (n 309) 43–44.
[343] The basic rule to transfer personal data in a third country was the existence of an "adequate level of protection" in the receiving country. The latter had to be assessed and confirmed by the EU Commission with an "adequacy decision". However, a list of possible alternatives was also included (e.g., conclusion with the party located in the third country of standard contractual clauses). See further, Paul M Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 8 Iowa Law Review 471.

international instruments, most of these provisions could already be found, to a less or greater extent, in the European landscape.

- **Data Subject's Consent -** Consent had a central role already in the Commission's DPD Proposal. Initially, the Proposal included the consent requirement in one comprehensive provision, that took the title of "Informed Consent"[344]. The provision detailed the conditions of consent ("specific and express") and listed the information that had to be provided to data subjects before their consent was collected[345]. In the final DPD version, however, the norm was subject to significant reformulations and its contents unpacked and distributed into different provisions. To clarify the meaning of "consent" under the directive, a definition was included which described consent as «*any freely given specific and informed indication of his* [the data subject's] *wishes by which the data subject signifies his agreement to personal data relating to him being processed*»[346]. The term "express" was deleted and any reference to the information that had to be provided to the data subject removed[347]. Under the DPD, the consent of the data subject represented the general condition to legitimise processing operations (the «unambiguous data subject's consent», Article 7), while alternative legal grounds (e.g., performance of a contract, legal obligation, public interest) included in the Directive were understood as exceptions[348]. The requirement of consent was also designated as a special condition in certain contexts (e.g., the "explicit" consent for processing of sensible categories of data[349] and the consent of the data subject to allow the transfer of his data in the absence of an adequate level of protection in the third country[350]). The meagre provisions of the DPD were supplemented in the following years with further indications, issued in particular by the Article 29 Working Party ("WP29")[351] (the advisory body established by the DPD and formed by representatives of the data protection authority of each EU Member State), in order to ensure a common application across Member States. Great emphasis was placed on the "active" behaviour of the data subject, since a

[344] Article 12 of European Commission, 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data' (n 315)., which was included among the "rights of the data subjects".
[345] The latter requirement was interpreted as indicating also an explicit concern. See Kosta (n 93) 89.
[346] Article (2)(h) of the DPD.
[347] See Kosta (n 93) 93.
[348] Pizzetti (n 318) 82; Fiona Carlin (n 314) 66.
[349] Article 8(2)(a) of the DPD.
[350] Article 26(1)(a) of the DPD.
[351] Following the 2016 data protection reform, the Article 29 Working Party was replaced by the European Data Protection Board ("EDPB"). However, many of its opinions remain a useful instrument of guidance.

genuine «*indication of …wishes*» required the person concerned to perform some kind of action, namely «*any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes*»[352]. Further the WP29 stressed the necessity for data subjects to be free from deception, intimidation, coercion or significant negative consequences in order for their choice to be authentic (i.e., "freely given")[353], and the importance of providing individuals with information clearly explaining the exact purposes of processing, for the choice to be conscious[354]. "Unambiguity"[355] and "explicitness"[356] of consent were also necessary elements, as they further confirmed the individual's intentions in providing his authorization. Freedom to provide consent translated also in the possibility for data subjects to withdraw it at any time, although this provision was not expressly included in the DPD[357] and was inferred by interpretation from the general construction of consent.

- **Information to be given to the data subject -** The DPD set forth specific transparency obligations that imposed on controllers a duty to provide data subjects with some basic details on data processing that involved personal data concerning them (usually contained in a document defined "privacy notice" or "privacy policy"). The provision was designed to ensure that individuals were informed and aware of the main elements of controllers' activities and uses of their data, and applied regardless of whether "informed" consent or another legal basis was required[358]. The DPD distinguished between two sets of information: (i) "essential information", namely the identity of the controller and of his representative, if any, and the purposes of the data processing[359]; and (ii) possible "further information", including the recipients of the data; the response obligation, and the existence of access and

[352] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (13 July 2011) WP187 11.
[353] The WP29 paid particular attention to consent in the employment context, as an example of a case in which the data subject is under the influence of the data controller. ibid 12–16.
[354] ibid 17–20.
[355] According to the WP29 "unambiguous" calls for the use of mechanisms to obtain consent that leave no doubt as to the individual's intention to provide consent. In practical terms, this requirement enables data controllers to use different types of mechanisms to seek consent, ranging from statements to indicate agreement (express consent), to mechanisms that rely on actions that aim at indicating agreement. ibid 21–25.
[356] "Explicit consent" is understood as having the same meaning as "express" consent. It encompasses all those situations in which individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. ibid 25–26.
[357] ibid 30.
[358] Pizzetti (n 318) 86–87.
[359] Article 10, let. a) and b) of the DPD.

rectification rights[360]. The additional information had to be provided, having regard to the specific circumstances in which the data were collected, if necessary «to guarantee fair processing having regard to the specific circumstances in which the data are collected»[361]. However, the leeway Member States were granted in the application of this norm resulted in privacy notices with varying degrees of comprehensiveness, depending on the applicable national law.

In terms of timing at which privacy notices needed to be provided, the DPD did not include any specific time indication for the case in which personal data were collected directly from the data subject. However, it was common understanding that the information had to be provided *before* or at most *at the time* of collection[362]. An express provision was instead included for situations in which data were communicated by a third-entity (company, authority, other subject), in which case the data subject needed to be informed «at the time of undertaking the recording of personal data»[363].

- **Right to access –** Article 12 of the DPD laid down the right to access, always considered one of the backbones of the data protection framework[364]. The right could be actually broken down in a bundle of sub-rights that enabled data subjects to obtain from data controllers «without constraint, at reasonable intervals and without excessive delay or expense»: (i) a *confirmation* as to whether or not data relating to them were being processed and a set of basic information on the processing[365]; (ii) the *communication* of his data in an intelligible form; and (iii) *knowledge of the logic involved in automatic data processing*, or at least those that involved automated decision-making processes[366]. The right to access encompassed also the right to request the rectification, erasure or blocking of data whose processing did not

[360] Article 10, let. c) of the DPD.
[361] Art. 10 of the DPD, see also Article 29 Data Protection Working Party, 'Opinion 10/2004 on More Harmonised Information Provisions' (25 November 2004) WP 100 7.
[362] Bygrave (n 14) 352.
[363] Art. 11(1) of the DPD stated that the notice with the necessary information could be provided «at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information».
[364] Pizzetti (n 318) 88.
[365] Article 12(a) and recital 41 of the DPD, the minimum set of information included at least the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data were disclosed.
[366] According to Bygrave there is no doubt this was inspired by Art. 3 of the French *Loi Informatique* of 1978, Bygrave (n 14) 353.

comply with the provisions of the DPD (e.g., because inaccurate or incomplete)[367]. The contents of these rights mirrored essentially the contents of the cousin rights, already variously included in national legislations.

- **Right to object –** This right entitled data subjects to oppose to specific data processing, therefore to stop it and prevent the controller to further use their data, under two main scenarios. When the processing was based on the controller's legitimate interest or on the performance of a task in the public interest, according to the DPD, data subjects could object to the processing of personal data «at any time *on compelling legitimate grounds*» relating to their particular situation[368]. Therefore, it required individuals to provide specific reasons to ground and justify their opposition.

  The second scenario, instead, concerned the possibility of data subjects to object to the processing of personal data for direct marketing purposes or third-party marketing purposes[369]. In this case, no justification was needed and the request had to be fulfilled with no further delay.
- **Automated decision-making processes -** Article 15 stipulated the right of individuals not to be subject to automated decision-making processes, namely decisions that produced «legal effects concerning him [*the data subject*] or significantly affects him» and had been taken based solely on automated means of processing[370]*.* Provisions along the lines of Art. 15 were relatively new in the European landscape, even though a handful of countries already included them in their domestic legal systems[371]. The scope of application of Art. 15 was subject to the fulfillments of four cumulative conditions: (i) the existence of a decision; (ii) with legal or significant effects; (iii) based solely on automated means and (iv) intended to evaluate particular personal aspects of the data subjects. The provision was considered an essential mean of empowerment against profiling practices[372].

[367] Article 12(b) of the DPD.
[368] Article 14(a) of the DPD.
[369] Article 14(b) of the DPD.
[370] In two cases Member States could subject individuals to automated decision-making data processing, namely when the process was: (i) necessary for the performance of a contract; or (ii) authorized by law, provided in both cases that adequate safeguards were implemented.
[371] Section 2 of the *Loi informatique* 1978, which is at the roots of this provision, along with Art. 12 Spanish data protection law of 1992 and Art. 16 of the Portuguese data protection law of 1991. Alessandro Bellavista, 'Art. 17' in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), *La tutela dei dati personali: commentario alla L. 675-1996* (2. ed, CEDAM 1999) 229–230; Bygrave (n 14) 320.
[372] See Bygrave (n 2) 321–327.

However, the manifold uncertainties that surrounded its interpretation and the fulfilment in practice of the mentioned conditions[373], deeply affected its successful implementation.

INSTITUTIONAL CONTROL – Alongside the mentioned subjective rights, the DPD included specific institutional control mechanisms that cantered mainly around the role and powers of public supervisory bodies. In particular:

- **Supervisory authorities –** The DPD required each Member State to appoint one or more independent public supervisory authorities, with the task to monitor the domestic application of data protection law[374]. The provisions on supervisory authorities were not particularly rich and left wide margins of appreciations to domestic systems. They included some general indications on the categories of powers these authorities had to be endowed with to perform their tasks, including investigative powers and effective powers of intervention (such as ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller)[375]. These authorities had also the duty to hear claims lodged by data subjects concerning the protection of their rights and freedoms with regard to the processing of their personal data. The DPD confirmed the role of supervisory authorities as privacy watchdogs of data protection in the European framework[376] and mildly attempted to harmonize their tasks and powers across Member States.
- **Notification and prior-checking –** The DPD devoted an entire section to notification requirements and prior-checking obligations. As a general rule, data controllers were required to notify the respective supervisory authority «before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes»[377]. The practice resembled the licensing schemes introduced in several domestic legal systems in the 70's and 80's, with some significant streamlining. In particular, contrary to most licensing regimes, this procedure did not require a specific authorization of the supervisory authority: upon notification, the processing operation

[373] See Bellavista (n 359) 228–229.
[374] Article 28 of the DPD, see further Roberto D'Orazio, in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), *La tutela dei dati personali: commentario alla L. 675-1996* (2. ed, CEDAM 1999) 367.
[375] Article 28(3) and recital 63 of the DPD.
[376] Pizzetti (n 318) 117.
[377] Article 18(1) of the DPD.

could be performed[378]. It allowed nonetheless supervisory authorities to receive a number of information (listed in the DPD) on ongoing processing activities that could facilitate their monitoring activity. The notified operations had to be included in a specific register under the supervision of the authority, open to consultation by the public or by any person demonstrating a legitimate interest[379]. As a further way of lightening a possibly burdensome requirement, the DPD laid down a number of derogations that allowed Member States to introduce simplifications or exemptions to such procedure[380]. This resulted substantially in Member States relying on the mentioned derogations to disregard the implementation of this mechanism[381], leaving the norm an empty shell.

More akin to a proper licensing scheme was the prior-checking mechanism envisaged by Article 20 DPD. The measure was addressed to «processing operations *likely to present specific risks* to the rights and freedoms of data subjects» that may derive from the risky nature of the processing operation, its broad scope or intrusive purposes. The selection of the processing operations that met the high-risk threshold and fell under the prior-checking obligation were left to the discretion of Member States. Some translated the provision into domestic pre-authorization procedures, by which controllers were required to notify a processing operation to their local data protection authority, before commencing it, and wait the approval of the authority (possibly contingent upon the implementation of additional safeguards) before initiating the process[382]. If a processing did not pass the assessment of the authority, the provision was generally interpreted in the sense of allowing data protection authorities to impede the starting of that data processing activity[383].

[378] Bygrave (n 14) 75.
[379] Article 21(2) and Recital 50 of the DPD.
[380] Article 18(2), (3), (4) and (5) of the DPD. Exemptions or simplifications could relate to categories of processing operations which were unlikely to affect adversely the rights and freedoms of data subjects; when the controller appointed a personal data protection officer; for public registers; or processing carried out by associations or foundations.
[381] Pizzetti (n 318) 98. Giovanni Battista Gallus, in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), *La tutela dei dati personali: commentario alla L. 675-1996* (2. ed, CEDAM 1999) 70–71. The Italian law implementing the DPD had introduced similar notification obligations as those provided for by the DPD, despite abandoning them a few years later.
[382] Art. 17 of the Italian Code introduced a “preliminary verification” procedure.
[383] Bygrave (n 14) 76. The combined reading of Art. 28(3), 20, recitals 9,10 and 54 DPD.

	Interests protected	Participatory control	Institutional control
Directive 95/46/EC	- Fundamental rights and freedoms of natural persons, and in particular their right to privacy - Free flow of information	- Data subject's consent - Right to information - Right to access (+ rectification and erasure) - Right to object / to be subject to an automated decision-making process	- Supervision by Data Protection Authority - Notification procedure - Prior-checking

Table 8. Directive 95/46/EC

5.2 A new fundamental right to data protection: Art. 8 of the Charter of Fundamental Rights of the European Union

The adoption of the Charter of Fundamental Rights of the European Union ("EU Charter") in 2000 marked another milestone in the history of data protection. Fundamental rights were already long considered an integral part of the general principles of the European legal framework[384] and were applied by the ECJ on the basis of existing international treaties (in particular the ECHR) and constitutional traditions of Member States[385]. With a view to reinforce the EU commitment to fundamental rights, in 1999 the European Council decided that a codified catalogue of fundamental rights of the EU should be adopted[386] in order «to make their overriding importance and relevance more visible to the Union's citizens»[387] and to consolidate them at EU level. A

[384] The statement that respect for fundamental rights formed «an integral part of the general principles of law protected by the Court of Justice» was clearly affirmed by the ECJ in the landmark decision of the *Solange I* case (*Internationale Handelsgesellschaft mbH v. Einfuhr und Vorratsstelle für Getreide und Futtermittel*, Case 11/70, [1970]), preceded by the *Stauder* decision, in which the ECJ had already hinted at the fact that fundamental human rights were «enshrined in the general principles of Community law» (*Stauder v City of Ulm,* Case 29/69, [1969]). See Mattias Kumm, 'Internationale Handelsgesellschaft, Nold and the New Human Rights Paradigm' in Miguel Poiares Maduro and Loïc Azoulai (eds), *The past and future of EU law: the classics of EU law revisited on the 50th anniversary of the Rome Treaty* (Hart 2010).

[385] Valeria Piccone and Oreste Pollicino (eds), *La Carta dei diritti fondamentali dell'Unione europea: efficacia ed effettività* (Editoriale scientifica 2018); Eleanor Spaventa, 'Fundamental Rights in EU Law' in Catherine Barnard and Steve Peers (eds), *European union law* (Oxford University Press 2017); Bruno De Witte, 'The Past and Future Role of the European Court of Justice in the Protection of Human Rights' in Philip Alston, Mara R Bustelo and James Heenan (eds), *The EU and human rights* (Oxford University Press 1999).

[386] European Council Decision on the drawing up of a Charter of Fundamental Rights of the European Union, in Annex IV to the Presidency Conclusions, 3 and 4 June 1999.

[387] Cologne European Council, 3-4 June 1999, Conclusions of the Presidency, at points 44-45 and Annex IV. The Convention included 15 representatives of the Heads of State and Government, 30 representatives of the national parliaments, 16 representatives of the European Parliament and 1 representative of the Commission.

special European Convention, composed by representatives of Member States, the EU Commission and the Parliament, was formed to draft the EU Charter, which was formally proclaimed in 2000 at the European summit in Nice[388]. While initially the EU Charter had a mere political value, with the entry into force of the Lisbon Treaty in 2009, the Charter acquired the same legal value of EU primary law[389].

One of the most innovative aspects of the EU Charter was the inclusion of a stand-alone "right to data protection" that acquired in this way the status of independent fundamental right of the European Union. The codification of a "new" right had been subject to a heated debate during the drafting stages of the EU Charter, especially due to the opposition of those that interpreted the tasks of the Convention as strictly limited to render more visible fundamental rights already existing under national constitutional traditions[390]. Therefore, initial proposals had tried to advance alternative options, including the idea to include a right to informational self-determination[391], to qualify data protection as a mean to safeguard identity, human dignity and confidentiality[392], or to incorporate a reference to data protection under the right to respect for private life[393]. However, they did not meet with general approval and were in the end all rejected. Eventually, the Convention agreed it was more appropriate to include a separate provision recognizing a right to the "Protection of personal data" and introduced it under Art. 8 after, right after Article 7 that enshrines the cousin right to "Respect for private and family life". A peculiar aspect of Art. 8 is that, according to the Explanations to the EU Charter, the main inspiration behind its introduction sprang from existing provisions of secondary EU law (in particular Directive 95/46/EC) and international instruments (Convention 108)[394], whose influence is clearly traceable in the wording and contents chosen by the EU Charter's drafters. After affirming, in the first paragraph, that

[388] Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 1. The Preamble of the Charter states that it reflects «common values» and reaffirms «the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, [...] and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights».
[389] See Article 6(1) and (2) Treaty on the European Union, and Article 51 of the EU Charter.
[390] González Fuster (n 59) 192.
[391] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 17.
[392] González Fuster (n 59) 195–197.
[393] ibid.
[394] As noted by Gonzales, however, neither of these instruments explicitly mentioned a "right to personal data protection", and on the contrary linked data protection rules to the safeguard of other fundamental rights and freedoms (e.g., the right to privacy). ibid 206.

«everyone has the right to the protection of personal data concerning him or her», the second and third paragraphs of Art. 8 crystalize the core elements of the new right, drawing from the key principles encapsulated in the DPD and Convention 108. Specifically, the second paragraph establishes that personal data have to be processed (i) fairly (ii) for specified purposes and (iii) on the *basis of the consent* of the person concerned or some other legitimate basis laid down by law. Further, it affirms *everyone's right* (iv) to have *access to his/her data* (v) and to *have this data rectified*[395]. Finally, in the third paragraph, Article 8 states that «compliance with these rules shall be subject to control by an independent authority». Of these six components, three are dedicated to the *proactive role of the individual* in the processing of their data. The elements of "consent of the person concerned"; "right of access to data" and "right to have data rectified" are thus elevated to core constituents of the fundamental right to data protection, corroborating the essential role of individuals as active participants in the data governance framework. Even though it never mentions it explicitly, the EU Charter confers undisputed prominence to individual self-determination. At the same time, the fact that Art. 8 lists a number of additional constitutive elements has led some authors to underline that the essence of this right should not confined to the individuals' ability to control their data, which represents only one specific facet[396].

5.3 Regulation (EU) 2016/679: the General Data Protection Regulation

5.3.1 Historical context and preparatory works

Despite its good intentions, the DPD did not really leave up to the expectations in harmonizing data protection within the EU[397]. Two reports published in 2003[398] and 2007[399] by the EU Commission on the implementation of the DPD[400] highlighted a

[395] See further on Art. 8 of the EU Charter, Oreste Pollicino and Marco Bassini, 'Sub Art. 8' in Roberto Mastroianni and others (eds), *Carta dei diritti fondamentali dell'Unione europea* (Giuffrè editore 2017) 136.
[396] Oreste Pollicino, 'Un Digital Right to Privacy Preso (Troppo) Sul Serio Dai Giudici Di Lussemburgo? Il Ruolo Degli Artt. 7 e 8 Della Carta Di Nizza Nel Reasoning Di Google Spain' in Giorgio Resta and Vincenzo Zeno-Zencovich (eds), *Il diritto all'oblio su Internet dopo la sentenza Google Spain* (RomaTrePress 2015) 12.
[397] Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer Berlin Heidelberg 2017) 2.
[398] European Commission, 'Report from the Commission. First Report on the Implementation of the Data Protection Directive (95/46/EC)' (2003) COM(2003) 265 final.
[399] European Commission, 'Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive' (2007) COM/2007/0087 final.
[400] Art. 33 of the directive required the EU Commission to report to the Council and the European Parliament on the implementation of the DPD, attaching to its report, if necessary, suitable proposals for amendments.

number of issues relating to the differences that persisted in national laws implementing the directive[401]. Rapid technological developments and globalization exacerbated this situation and posed fresh challenges to the protection of data that did not find adequate answers under domestic policies. Due to a mounting pressure to act, in 2009 the EU Commission launched a public consultation[402] that explored the need to amend the existing legal framework on data protection and asked for input on future measures to address the impacts of new technologies[403]. Following the reactions of private and public stakeholders[404], which confirmed the need to develop and adapt existing data protection rules to the new digital reality, in November 2010 the EU Commission set out its strategy to modernize the EU data protection framework, publishing a communication that outlined the envisaged "comprehensive approach on data protection in the EU"[405]. Key objectives of this approach were (i) the strengthening of individuals' subjective rights; (ii) the enhancement of control over their own data, and (iii) the protection of free and informed consent. According to the EU Commission, «the retention by data subjects of an *effective control over their own data*»[406] was an essential precondition of a high level of data protection. It also recognized that the achievement of this individual control had become «particularly challenging in the online environment, where data are often retained without the person concerned being informed and/or having given his or her agreement to it»[407]. As a consequence, the Commission urged a swift action to reinforce the position of data subjects vis-à-vis data controllers; improve existing rights and introduce additional ones.

---

[401] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 25.

[402] The public consultation was from July to December 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm). The EU Commission launched a second public consultation from November 2010 till January 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm), after its strategy was published to gain further feedback and comments.

[403] Information available at: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm (last accessed 31 May 2014).

[404] Notably the Article 29 Data Protection Working Party and Working Party on Police and Justice (n 11).

[405] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' (n 11). ibid 7. See also V Reding, 'The Upcoming Data Protection Reform for the European Union' (2011) 1 International Data Privacy Law 3, 3–5.

[406] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' (n 11) 7.

[407] ibid.

In January 2012, after intense institutional discussions[408], the Commission presented its reform package to modernise the EU data protection framework[409], whose golden piece was the long-awaited regulation setting out a general EU framework for data protection and replacing Directive 95/46/EC[410]. Reinforcing effectiveness and individual control; adapting data protection rules to the digital single market and providing enhanced consistency across Member States were the main drivers of the reform[411]. The Communication opened up in its very first paragraph re-affirming that «in this new digital environment, *individuals have the right to enjoy effective control over their personal information*»[412] and dedicated an entire section to "Putting individuals in control of their personal data"[413], detailing the actions required to improve individuals' ability to control their data and strengthen their right to data protection. The proposal for a new general data protection Regulation was subject to tough negotiations and fierce discussions. After four years from its first presentation, on 4 May 2016, Regulation 2016/679 (UE) (General Data Protection Regulation, "GDPR")[414] was finally adopted to replace Directive 95/46/EC and became directly applicable from 25 May 2018.

5.3.2 The General Data Protection Regulation

OBJECTIVES – Under the GDPR, the dual purposes of the DPD – to ensure a consistent and high level of protection of natural persons and remove the obstacles to flows of personal data within the Union - remain sound[415]. However, the right-based

[408] See the European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (n 11).
[409] See ibid and; V Reding, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2 International Data Privacy Law 119.
[410] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' (2012) COM/2012/011 final-2012/0011 (COD). The package included also a directive setting out rules on the protection of personal data in the police and criminal justice sector, (European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data' (2012) COM/2012/010 final-2012/0010 (COD).) The latter directive is not covered by this work.
[411] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (n 11) 2–3.
[412] ibid 2.
[413] ibid 4–6..
[414] 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).
[415] Recital (9) of the GDPR.

approach to data protection finds in the GDPR new roots. Not only, thanks to the EU Charter, data protection had become an autonomous fundamental right of individuals, but Art. 16 TFEU[416] gave an express mandate to the European Parliament and the Council to «lay down the rules relating to the protection of individuals with regard to the processing of personal».

This new status is reflected in the very first recital of the GDPR[417], where the reference contained in the DPD to the protection of fundamental rights and freedoms of natural persons and «in particular their right to privacy»[418] is replaced by «their right to protection of personal data». The GDPR does not directly endorse nor refer to a right to informational self-determination. However, recital 7 states that «natural persons should have *control of their own personal data*» which, for the first time, expressly affirms the principle of individual control in a EU legal act.

MAIN PROVISIONS – The GDPR introduces a number of innovations that would be too long to summarize here and would take us off-topic from our core research purpose. Suffice to say that the choice of a regulation over a directive for the new data protection framework is certainly a major shift and reflects the intention of the European legislator to achieve greater harmonization and consistency in the Union. From a content perspective, despite a general sense of continuity with the DPD (the basic concepts and principles of the DPD continue to exist, subject to some clarifications and changes in detail[419]), some innovative aspects are also present. For example, a general "principle of accountability"[420] is now included in the GDPR, which burdens controllers with the responsibility to ensure that their processing activities are compliant with GDPR

[416] The introduction of Art. 16 in the Treaty on the Functioning of the European Union (TFEU), with the Lisbon Treaty, was part of the bigger European plan to make data protection a fundamental right in the EU. The article in its first paragraph restated the fundamental right nature of data protection, reinforcing Art. 8 of the EU Charter. In the second paragraph, it gave the European Union mandate to act for the protection of this right throughout the EU. It thus became the new legal ground on which data protection rules could be adopted. Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016).

[417] Recital 1 of the GDPR states that «the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her».

[418] Article 1(1) of the DPD.

[419] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 28.

[420] Giusella Finocchiaro, 'Il Quadro d'insieme Sul Regolamento Europeo Sulla Protezione Dei Dati Personali' in Giusella Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101* (Prima edizione, Zanichelli editore 2019) 19. A separate principle of accountability was already provided in the OECD Guidelines.

provisions and the ability to demonstrate said compliance[421]. The provision is strictly related to the new risk-based approach that permeates the GDPR, which links controllers' obligations to the level of risk that their activities may pose to data subjects' rights and freedoms[422]. The catalogue of data protection principles is further expanded, including an explicit recognition for the principle of "data minimization"[423], and new concepts are introduced, such as "privacy by design" and "by default"[424]. More generally, the GDPR introduces a range of new requirements that controllers need to comply with (e.g., the adoption of a record of processing activities[425], the appointment of a data protection officer "DPO"[426], the performance of a data protection impact assessment (DPIA)[427]); it strengthens data breach management procedures and further details the requirements for transferring personal data to third countries outside the EU[428]. The new body of rules is not drastically different, in terms of structure and contents, from the previous framework. But it certainly denotes an overall change of

[421] ibid 17–21. Voigt and Von Dem Bussche (n 397) 31–33.

[422] Alessandro Mantelero, 'La Gestione Del Rischio' in Giusella Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101* (Prima edizione, Zanichelli editore 2019) 473 ff.

[423] Article 5(c) defined "data minimization" as the collection of data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. See Marco Dell'Utri, 'Principi Generali e Condizioni Di Liceità Del Trattamento Dei Dati Personali' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (G Giappichelli editore 2019) 209.

[424] Article 25 of the GDPR. See Ann Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-Makers and Policy-Makers* (Information and Privacy Commissioner of Ontario, Canada 2011); Fabio Bravo, 'L'«architettura» Del Trattamento e La Sicurezza Dei Dati e Dei Sistemi' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (G Giappichelli editore 2019) 790.

[425] Art. 30 GDPR requires controllers and processors to maintain a record of processing activities that needs to include certain basic information on the processing (such as a description of the data categories, purposes of processing, categories of recipients, implemented security measures). The record has to be kept up to date and disclosed in case of investigation. It is an essential starting tool for both controllers/processors and supervisory authorities to check and monitor the internal entity's compliance.

[426] Artt. 37-39 GDPR are devoted to define the characteristics, tasks and powers of the "Data Protection Officer" (DPO), a subject with advisory and monitoring role to ensure data protection compliance, as well as the cases in which the DPO needs to be appointed. The EDPB has provided extensive guidance on this figure, see Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' (13 December 2016) WP243rev.01 later endorsed by the EDPB.

[427] Art. 35 GDPR lays down indications on the performance of a "Data Protection Impact Assessment" (DPIA), listing the high-risk cases in which a DPIA is required by law (e.g., in case of large-scale data processing, systemic monitoring or systemic and extensive evaluations of personal characteristics) and the information a DPIA needs to contain to prove a correct assessment. See further Article 29 Data Protection Working Party, '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) WP248rev.01. A detailed analysis of the DPIA is conducted under Chapter IV.

[428] The comprehensive system of rules that governs transborder data transfers outside the EEA is laid down under Articles 45-49 GDPR, that detail a layered regime of safeguards that controllers need to comply with in order to legitimize a transfer of personal data.

attitude[429]. The risk-based approach of the GDPR re-shapes the organizational model: data controllers are placed at the very centre of the data governance ecosystem and are entrusted with most of the choices, the assessments and the control powers over data processing.

PARTICIPATORY CONTROL – One of the goals declared by the Commission's Proposal was to make «data protection *more effective in practice*»[430], also by mean of reaffirming of users' control over their data. The rights of the data subjects provided for in the DPD have all been confirmed in the GDPR, and have been further clarified, strengthened or even extended. With a view to avoid repetitions, only the main novelties of GDPR provisions compared to the previous framework are examined below. Also, as previously indicated, references to the provisions of the e-privacy Directive are included, where relevant to our analysis.

- **Data subject's consent -** The basic concept and role of consent is similar to the one envisaged in the DPD. Consent remains one of the legal bases that legitimize the processing of personal data[431], in general, and derogate from the prohibition to process special categories of data[432]. The requirements of a "free", "specific", "informed" and "unambiguous indication of the data subject's wishes" are also confirmed[433]. Each of these aspects has been subject to extensive clarifications by the WP29, first, and the European Data Protection Board ("EDPB")[434], later, that building up on previous opinions[435] have provided additional insights and examples

[429] Finocchiaro, 'Il Quadro d'insieme Sul Regolamento Europeo Sulla Protezione Dei Dati Personali' (n 420) 2.
[430] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 29.
[431] Art. 6 GDPR lists the legal grounds that legitimize a data processing to be carried out. The data subject's consent is the first legal basis mentioned in the article (Art. 6(1)(a)).
[432] Art. 9 GDPR, which deals with the processing of "special categories of data" (namely data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data), includes a general prohibition to process this data unless one of the listed conditions is met, among which is included the data subject's «explicit consent to the processing» (Art. 9(1)(a)).
[433] Art. 4(11) GDPR defines the "consent of the data subject" 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 definition consent».
[434] The EDPB is the European independent body, composed of representatives of the 27 EU and 3 EEA EFTA national data protection authorities, and the European Data Protection Supervisor (EDPS). Established by Art. 68 of the GDPR, the EDPB takes the place, functions and powers of the previous WP29.
[435] See notes 352 and ff. above, on the clarifications provided by the WP29 on the notion and requirements of consent under the DPD.

on their meaning and practical application[436]. Renewed emphasis is placed on the fact that consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms presented, without enduring negative consequences[437]. Scenarios of imbalance of power (e.g., in the relationship with public authorities or employers)[438] and "conditionality"[439], namely the case in which the provision of a service is "tied" to the provision of a consent to processing personal data that are not necessary for its execution (e.g., ad purposes), are subject to particular scrutiny, since they represent situations in which it is generally presumed the consent cannot be freely given.

The efforts of the GDPR to provide more detailed and practical indications, compared to the previous framework, is reflected also in the increased attention paid to the modalities in which consent requests needs to be presented and consent further collected. The GDPR devotes to the "presentation" aspect a specific paragraph under Art. 7, which requires consent forms to be provided to data subjects in a clear and distinguishable way, with intelligible forms and using clear and plain language[440]. On the second aspect, the existence of a *proactive* and *unambiguous* behaviour of the person, as indisputable sign that the individual wanted to provide his approval, remain two key assessment criteria for a valid consent. In particular, in its new definition, the is linked to the provision of a "statement" or in any case a "clear affirmative action", thus implying that a person must take a deliberate act or maintain an active behaviour[441]. Silence and inactivity do not meet the intentionality threshold required for valid consent, but also mechanisms of scrolling or swiping through a webpage can hardly be considered authentic manifestations of choice, unless proven otherwise[442].

---

[436] Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (8 April 2018) WP259rev.01 which were endorsed by the EDPB at is first Plenary meeting and slightly updated with Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020.

[437] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020) 7; Fabio Bravo, 'Le Condizioni Di Liceità Del Trattamento Di Dati Personali' in Giusella Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101* (Prima edizione, Zanichelli editore 2019) 151–155.

[438] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 437) 8–9.

[439] ibid 10–11.

[440] Recital 42 and Article 7 GDPR.

[441] Art. 4(11) GDPR specifies that valid consent requires «an unambiguous indication by means of a statement or by a clear affirmative action». Recital 32 sets out additional guidance on this, providing that consent can be collected through a written or (a recorded) oral statement, including by electronic means.

[442] Recital 32; European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 437) 18–19; Fausto Caggia, 'Libertà Ed Espressione Del Consenso' in Vincenzo Cuffaro,

With reference to the requirement of "explicit" consent[443], the latter remains confined to particular situations that demand for a higher standard of proof of the will of the data subject. "Explicit" consent is still central in the processing of special categories of data (a role in Article 9) and, most notably, it is incorporated in Article 22, where it acts as one of the conditions that legitimize automated decision-making processes, including profiling[444]. Specific rules on consent are also introduced in the context of information society services. The easy accessibility and dissemination of online services requires an additional layer of protection where personal data of vulnerable subjects, like children, are collected[445].

Finally, contrary to the DPD, the right to withdraw the previously provided consent, easily, free of charge and without detriment, acquires a prominent place in the GDPR[446] and is confirmed as a necessary condition for the validity of consent itself[447].

These general rules defining the characteristics of a valid consent apply now equally to cases in which the consent of the data subject is required under the e-Privacy Directive (*lex specialis* with respect to the GDPR)[448], where this legal basis plays a pivotal role when it comes to the processing of personal data in the context of electronic communications. Consent is in fact a necessary pre-condition for most of

---

Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (G Giappichelli editore 2019) 260; Bravo (n 437) 155.

[443] Despite some ambiguities in the clear distinction between "unambiguous" and "explicit" consent, according to the EDPB the term "*explicit*" hints to a more rigorous consent manifestation, as it means that the data subject *must give an express statement of consent*, which usually implies a *confirmation in a written form*. The EDPB lists other possible ways in which the requirement is met, such as issuing the required statement «by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature». European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 437) 20–21.

[444] In art. 22 of the GDPR the explicit consent of the data subject is one of three conditions (the other being the performance of a contract or the authorization by law) that avoid the application of the general right of the data subject not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her.

[445] Art. 8 GDPR lists the conditions applicable to children's consent in relation to information society services.

[446] Caggia (n 442) 268; Bravo (n 437) 157–164.

[447] Article 7(3) GDPR, see also European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 437) 23–24.

[448] To dispel any doubt, the EDPB provided extensive clarifications on the interplay between the e-Privacy Directive and the GDPR, confirming their *lex specialis – lex generalis* relationship. Therefore, the general rules (e.g., conditions for a valid consent) established by the GDPR apply, except for situations where the e-Privacy Directive "particularises" (i.e. renders more specific) the rules of the GDPR (e.g., cases in which consent is required), where the e-Privacy Directive shall take precedence. European Data Protection Board - European Data Protection Supervisor, 'Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities' (12 March 2019).

the processing activities covered by the directive[449], including the use of cookies and other tracking technologies, as well as the processing of users' contact details for marketing purposes (with very few exceptions)[450]. Particularly with respect to the "cookie consent", the e-Privacy Directive already stressed the need to ensure an active behaviour of the consenting data subject (e.g., by «ticking a box when visiting an Internet website»[451]), as later reaffirmed by the GDPR.

In brief, the GDPR does not substantially change the rules or requirements of consent already provided for in the DPD. It codifies them in plainer terms and particularizes them with further details, narrowing the chances for divergent applications. Compared to an earlier tendency that elevated consent to general condition of processing activities, the GDPR seems to recalibrate its role, assigning it a weight equivalent to the other several legal grounds of processing.

- **Information obligations –** In the GDPR, transparency of data processing is the first of the basic principles of data processing (Art. 5(a))[452]. The obligations of data controllers to inform data subjects, and the consequent right of data subject to obtain such information, continue to have a central role in the new framework, as primary instruments to ensure the awareness, thus empower, data subjects. Compared to the DPD, the distinction between the sources from which information can be collected (from the data subject or a third entity) and between categories of information ("minimum set" and "additional" information) are maintained. However, the margin of discretion of Member States to decide which information needs to be provided to the data subject is removed and the list of elements is considerably expanded and detailed[453]. Filling the gap left by the DPD, the GDPR indicates the

[449] In particular, according to the e-privacy Directive, consent is necessary for: (i) storing information and gaining access to information stored in the terminal equipment of the user (by means of cookies, web bugs, fingerprints and similar tracking technologies) and (ii) processing traffic data for the purpose of marketing electronic communications; to (iii) processing location data in the provision of value-added services and including subscribers in public directories; (iv) processing of personal data for purposes of direct marketing via automatic calling systems, fax, e-mail, SMS, MMS or similar methods.

[450] These include the so called "soft spam" exception, whereby email marketing communications can be sent to a data subject without his previous consent, provided the contact details were collected in the context of a previous purchase with the sender and the communication concerns the promotion of products or services similar to those of the original purchase.

[451] Recital 17 of the e-Privacy Directive stating: «[…] consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website».

[452] Art. 5(a) GDPR pairs the transparency principle with the principles of fairness and lawfulness of data processing, stating that data needs to be «processed lawfully, fairly and in a transparent manner in relation to the data subject»

[453]Articles 13 and 14 GDPR include also: the details of the DPO, the legitimate interest of the controller (when this is the legal basis), the categories of recipients and the intention to transfer data to third

time at which information needs to be communicated to data subjects (at the latest "at the time of collection")[454]. In addition, to avoid that transparency rules are treated as a formality, the GDPR requires that the information notice needs to be provided in concise form, easily accessible, and easy to understand, using clear and plain language[455].

The same information obligations are laid down also in the e-Privacy Directive, which largely mirror the transparency requirements provided by general data protection rules, making either direct reference to the contents of the DPD (now to be intended as a reference to the GDPR)[456], or listing the required information in the text of the norm[457].

- **Right of access, right to rectification, right to erasure ("right to be forgotten"), right to restriction of processing –** As opposed to the DPD, where the right to rectification, erasure, and blocking fell under the broader umbrella of the right to access, in the GDPR each of these rights has a separate provision. Access to personal data, however, remains a cardinal and prodromic right for the successful exercise of all the others[458]. The scope and meaning of these rights are not radically revised, but the new norms are more rigorous in the indication of the conditions to which these subjective rights can be exercised, and in the list of exceptions that data controllers can raise to trump data subjects' requests[459].

  The right to access is broken down into minor sub-rights that mirror those already included under the DPD (i.e., have confirmation of whether personal data are being processed and receive a series of elements on the processing activities; as well as

countries. Annarita Ricci, 'I Diritti Dell'interessato' in Giusella Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101* (Prima edizione, Zanichelli editore 2019) 393–394.

[454] Article 13(1) of the GDPR.

[455] Recital 53 GDPR; Ricci (n 453) 395.

[456] In the context of the storing or gaining access to information in the terminal equipment of a subscriber or user, Article 5(3) provides that the user and subscriber must have «been provided with clear and comprehensive information, in accordance with Directive 95/46/EC [*now GDPR*], about the purposes of the processing».

[457] This occurs in particular in relation to traffic data and location data. According to Article 6(4), before the collection of traffic data, users need to be informed on «the types of traffic data which are processed and of the duration of such processing». Similarly, Article 9(1) on location data states that users «must inform of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value-added service».

[458] Giuseppe Di Genio, 'Trasparenza e accesso ai dati personali' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), *La nuova disciplina europea della 'privacy'* (Wolters Kluwer 2016) 170.

[459] Ricci (n 453) 397.

obtain a copy of the personal data)[460]. According to some authors, the right to access should give data subjects the possibility to demand more detailed information on processing than those usually contained in privacy notices, as the right should be designed to permit an in-depth assessment over lawfulness of the controller's activities[461]. The rights to rectification, erasure, and restriction[462] continue to be instrumental primarily to correcting or blocking unlawful data processing that result from incomplete and inaccurate data, or excessive retention periods[463]. Among the latter, the right to erasure was certainly the one to receive the most attentions, also in light of the lively doctrinal and jurisprudential debate that sprang on the scope of application of this new right, particularly in the digital context (also referred to as "right to be forgotten")[464]. While different meanings have been attributed to this right over time ("not to see published news of events after a considerable period of time" or a "right to contextualization")[465], it is generally agreed that it adapts the right erasure to the online environment, where it finds new forms of applications (e.g., in the context of search engines as a right to request the de-referencing/delisting of contents associated to the requester). This specification is now expressly covered under Art. 17 GDPR, which compels data controllers who receive a "forgotten"

[460] Art. 15 and recital 63 state that: «every data subject should therefore have the right to know and obtain communication» of information relating to the data processing (e.g., purposes, period of processing, recipients, the logic involved in any automatic personal data processing) and, where possible, «remote access to a secure system which would provide the data subject with direct access to his or her personal data».

[461] Recital 63, Voigt and Von Dem Bussche (n 397) 150.

[462] Respectively, Articles 16, 17 18 of the GDPR.

[463] Voigt and Von Dem Bussche (n 397) 154.

[464] The express recognition of a "right to be forgotten" had been under discussion in the European framework for quite some time and was already included in the 2012 Commission Proposal. In 2014, it hit the news with the notorious CJEU decision in the *Google Spain* case, in which the Court ruled out that an Internet search engine had to consider requests from individuals concerning the removal of links to freely accessible web pages, that resulted from web searches on their name, in accordance with the right to erasure granted to data subjects under data protection law. See Giusella Finocchiaro, 'La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems' (2015) 31 Diritto dell'informazione e dell'informatica 779. See also the European Data Protection Board, 'Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR' (7 July 2020).

[465] Giusella Finocchiaro, 'Il Diritto All'oblio Nel Quadro Dei Diritti Della Personalità.' in Giorgio Resta and Vincenzo Zeno-Zencovich (eds), *Il diritto all'oblio su Internet dopo la sentenza Google Spain* (RomaTrePress 2015) 30 ff. Others define it a "right to not be seen", Manuela Siano, 'Il diritto all'oblio in Europa e il recente caso spagnolo' in Franco Pizzetti (ed), *Il caso del diritto all'oblio* (G Giappichelli 2013) 132. or a "right to the downsizing of one's own telematic visibility", Salvatore Sica and Virgilio D'Antonio, 'La Procedura Di De-Indicizzazione' 2014 Diritto dell'informazione e dell'informatica 703.

request to inform also any other controller in the processing chain to abide to the request of erasure (including any links to, or copy or replication of the contents)[466]. Finally, for all these rights (as well as those described below), the GDPR provides specific indications on the modalities (in terms of timing, language, and possible charges) based on which data subjects' requests need to be handled properly[467].

- **Right to object:** compared to the DPD, the right to object in the GDPR is slightly improved and it is made easier for data subjects to exercise it successfully when data processing activities do not correspond to their will[468]. The scope of the right remains narrowly drafted and the scenarios in which the right to oppose can be exercised essentially reiterate the range of situations already established under the DPD, only supplemented with some additional clarifications[469]. Specifically, the data subject has the right to object in case of interest-based data processing (i.e., based on the legitimate interest of the controller or necessary for the performance of a task in the public interest), where the right arises from the existence of new circumstances that influence the initial balancing of interests due to a specific situation of the data subject[470]. In this case, contrary to the DPD's logic, that required the applicant to prove that his reasons prevailed on the legitimate interests of the controller, the GDPR demands controllers that want the turn down the request to demonstrate the compelling legitimate grounds that override the interests of the data subject and justify the continuation of the processing[471]. In addition, the right to block the use of personal data can be exercised when these are processed for research or statistical purposes, or for direct marketing purposes, when based on the controllers' legitimate interest (in the latter case with no ground to refuse on the part of data controllers)[472].

[466] The same obligation was already included in the DPD under the general article concerning the right to access (Art. 12), where, under let. (c), the DPD imposed on controllers an obligation of «notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking […] unless this proves impossible or involves a disproportionate effort».
[467] In particular, Article 12 of the GDPR provides that the response needs to be provided «without undue delay and in any event within one month of receipt of the request» and «in a concise, transparent, intelligible and easily accessible form, using clear and plain language». Ricci (n 453) 402–403.
[468] Voigt and Von Dem Bussche (n 397) 177.
[469] Article 21 of the GDPR.
[470] Voigt and Von Dem Bussche (n 397) 177.
[471] Ricci (n 453) 449.
[472] Art. 21(2) GDPR, which provides under certain circumstances an "opt-out" regime in the context of direct marketing, according to which controllers may perform direct marketing without the prior consent of the data subject, provided the latter is granted the possibility to object to (i.e., opt-out of) the processing, in an easy way, blocking the sending of any further commercial communication.

As for the e-Privacy Directive, broad application of the right to object could be found in particular before an amendment introduced in 2009[473], since up to that moment the use of cookies was regulated according to an "opt-out" regime. Based on this regime, websites could store profiling cookies and similar tracking technologies on users' terminal equipment without their consent, provided they were given an opportunity to refuse to have these technologies installed[474]. Following the 2009 amendment, an opposite "opt-in" model for cookies was introduced, that required users to express their consent, which in turn relegated the right to object of users to a narrower set of circumstances, in particular concerning the use of customers' electronic contacts (e-mail) for direct marketing purposes in the context of an established commercial relationship[475].

- **Automated decision-making processes –** As analysed above, a provision dedicated to "automated individual decisions" was already included in the DPD[476] and in at least some of national data protection laws[477]. The right of individuals not to be subject to decisions taken *solely* by machines and which produce legal or similar effects has actually some old roots. With the ever-evolving progresses in profiling techniques and machine-learning based technologies, the provision has acquired new relevance. In practice, however, the conditions that determine the application of this norm mirror those already established under the DPD, in particular the fact that the decision must produce "legal effects" or in any case "significantly affect" the data subject[478]. The express mention of "profiling" as one of the types of processing that could trigger the provision could already be found in the words of the Directive that referred to «automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability,

[473] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. ("Cookie amendment")
[474] Frederic Debusseré, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?' (2005) 13 International Journal of Law and Information Technology 70, 86–89.
[475] Article 13(2) e-Privacy Directive. See above note 450 on "soft spam" activities.
[476] Art. 15 of the DPD.
[477] See for example section 6 of the BDSG.
[478] Art. 22(1) GDPR and further clarifications provided with the Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (6 February 2018) WP251rev.01.

conduct»[479]. In sum, despite the centrality of this right in light of the growing adoption of machine-based decisions, its rationale and main components do not represent absolute novelties in the European landscape.

- **Right to data portability –** The codification of a "right to data portability" is probably the key innovative aspect in the context of subjective rights. Stemming as a peculiar ramification of the right to access, this right represents a key enabler of user control as it aims at facilitating the sharing and re-use of personal data among data subjects[480]. Essentially, the right to data portability seeks to rebalance the power dynamics between controllers and data subjects, providing the latter with a workable mechanism to obtain and re-use for their own purposes personal data that controllers hold about them. The provision entitles data subjects to (i) receive personal data «in a structured, commonly used and machine-readable format»[481]; (ii) and «transmit those data to another controller» or, where technically feasible, to «have the personal data transmitted directly from one controller to another»[482]. The objective is to reduce lock-in effects and enable data subjects to migrate data and switch service providers more easily, without their data being kept hostage[483]. The scope of application of the norm, however, remains quite limited as it applies only to data whose processing was based on the data subject's consent or on a contract[484].

INTISTUIONAL CONTROL – With respect to institutional control mechanisms, the GDPR adopts two different approaches. On the one hand, it simplifies existing requirements, with the intent to reduce costs for data controllers; on the other hand, it strengthens the role of supervisory authorities.

- **Notification procedures -** Compared to the DPD, prior notification and authorization procedures are largely eliminated or lightened[485]. The only prior consultation procedure left in the GDPR applies in a very narrow case-scenario, namely when, following the conduction of a data protection impact assessment and the application of appropriate mitigating measures, the risks resulting from the

[479] Art. 15(1) of the DPD.
[480] Ricci (n 453) 436; Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (5 April 2017) WP242rev.01.
[481] Article 20(1) of the GDPR, see further Voigt and Von Dem Bussche (n 397) 174.
[482] Article 20(3) of the GDPR, see ibid 175.
[483] Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480) 9.
[484] Art. 20 (1), lit. a) and b) of the GDPR.
[485] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (n 314) 29.

envisaged processing activities remain high[486]. Upon receiving a request of consultation, the DPA has to provide a "written advice", either giving a favourable opinion or indicating where the intended processing violates the regulation, with the possibility to exercise any of the corrective powers (among which warning controllers; specifying additional mitigating measures or banning the processing).

- **Data Protection Authorities –** Contrary to the DPD, which contained a poor amount of basic provisions, in the GDPR the role of supervisory authorities is enhanced, their tasks and powers considerably expanded and detailed[487]. The DPD's high-level wording is replaced with a detailed and varied list of responsibilities, as well as a dense set of investigative and corrective means that aim at strengthen the monitoring functions and enforcement powers of DPAs[488]. The GDPR reinforces also a number of cooperation and assistance mechanisms between supervisory authorities, with a view to ensure a consistent application of the GDPR throughout the Union[489].

  The role, tasks and powers of supervisory authorities will be dealt more closely under Chapter IV.

	Interests protected	Participatory control	Institutional control
Regulation (EU) 2016/679	- Art. 8 of the EU Charter (right to data protection) and other fundamental rights and freedoms - Free flow of personal data	- Data subject's consent - Right to information - Right to access - Right to rectification, restriction and erasure - Right to object - Right not to be subject to an automated decision-making process - Right to data portability	- Supervision by data protection authority - Limited prior consultation procedures

Table 9. Regulation (EU) 2016/679

[486] Article 36 of the GDPR, see also the Article 29 Data Protection Working Party, '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' (n 427).
[487] Pizzetti (n 318) 165.
[488] Respectively, Art. 57 GDPR on the "Tasks" and Art. 58 GDPR on the "Powers" of DPAs.
[489] See e.g., Articles 60-63 of the GDPR.

6 Wrapping up the analysis: comparative overview of the legal instruments

The analysis conducted in the previous paragraphs, starting in 1970 with the Hessen Data Act and ending in 2018 with the GDPR, provided an overview of the evolution of the data protection framework in the European context. Throughout this lens, the investigation has helped to outline the progressive consolidation of the idea of active control and participation of individuals in the processing and circulation of their personal data, elected among the distinctive features and underlying goals of modern data protection. From a comparative examination of the various data protection acts reviewed above, some concluding observations can be drawn.

EMERGENCE AND EXPANSION OF A PROACTIVE DATA SUBJECT – The analysis has shown how the idea of individuals being entitled to be active participants in data processing choices with a view to protect their privacy interests was not a primary concern of early national legislations governing automated processing activities. The first data protection instruments (national laws in Hessen and Sweden, but also the Resolutions (73)22 and (74)29 of the CoE) were mostly concerned with the protection of the collectivity from the abusive and wrongful employment of technologies, that provided governments with new capacities of monitoring and surveillance. Little room was instead reserved to individual privacy interests. These acts focused mainly on broad principles of good data governance (fairness and data quality above all), that were further translated into security and transparency requirements for public supervision. Envisaged “control mechanisms” over processing activities were largely of institutional nature and were centralized in the hands of newly established supervisory authorities. Individual rights were not totally absent, however in this first phase they had no real empowerment qualities as they served mainly to achieve other data processing principles (e.g., data quality). In essence, they had more of a social and collective function rather than protecting specific individual interests.

Participation and control of data subjects appeared to gain traction with the progressive shift towards a rights-based approach to data protection. From the ‘80s, both at national and international level, data protection started to be linked to the safeguard of a number of individual rights and freedoms, whose connection varied depending on the constitutional legal traditions of Member States (e.g., human dignity, autonomy, privacy, self-development, informational self-determination). The strict relationship between data protection rules and the safeguard of fundamental rights, such as autonomy, self-

development and self-determination, which presume a pro-active and involved individual, promoted the idea that data subjects had to be granted a certain degree of influence over the processing of personal data. In parallel, individuals themselves started to claim more involvement and control on decisions that concerned information relating to their identity, personality and life choices. Data protection began to be increasingly construed as a right designed to protect individuals by entitling them to control their own information, thus governing the modalities through which one’s private sphere/personality/identity is build.

The data subjects’ consent, considered the maximum expression of user control, was gradually considered an essential precondition to legitimise data processing activities, particularly in the private sector. The number and scope of other subjective rights that individuals could exercise to monitor and challenge the use of their personal data, even after having shared them with controllers, increased and expanded.

The trend towards stronger individual empowerment, already traceable at national level, since the first French *Loi Informatique* and German BGB, was formally recognized in leading international instruments like the 1980 OECD Guidelines and Convention 108, and it gained real momentum at European level, first with the implementation of the DPD, then with the GDPR. The inclusion of the right to data protection among the freedoms protected by the EU Charter, which marked its independence and definitive entry within the catalogue of EU fundamental rights and freedoms, codified the participatory role of individuals among its constituent elements.

INDIVIDUAL CONTROL AS A “BUNDLE” OF RIGHTS – A general principle of individual participation or control over personal data is rarely found in policy documents. One of the few exceptions are the OECD Guidelines (both in the 1980 and in the 2013 versions) that include a separate provision on the principle of “Individual Participation”. No other legal act in the history of data protection has formalized this idea in such explicit terms. A step towards a more visible recognition of this general notion of “control over personal data” was made in the EU policy document adopted during the data protection reform. that advocate for the empowerment of individuals and include explicit references to the right of individuals to “enjoy effective control over their personal information”. The same approach is reflected in the GDPR, where control makes a swift appearance in its recitals, failing however to join the other general data processing principles under Article 5. In the absence of a formal codification, the principle of control

of data subjects manifests itself in a combination of different provisions taking the form of a "bundle" of micro-rights. It is the number, scope and effectiveness of these micro-rights that define in practice the degree of control and participation data subjects are allowed to enjoy.

This bundle of subjective rights changed over time, both in quantity and contents. Some core rights (to access, erasure, and rectification) were present since the older data protection acts, even though they occupied a marginal position and were considered instrumental to the broader purposes of technology regulation. The trend in time shows, however, a continuous expansion in scope and range of subjective rights. These get increasingly detailed and easier to exercise. Data subjects' consent has gained momentum, becoming a cardinal condition to legitimize data processing (especially in the private sector). Transparency rights were raised to essential means of empowerment for individuals since, like consent, they provide individuals with an anticipatory form control, before data processing are initiated. Other rights, (e.g., to access, correct or update, and block data processing) that offer an *ex-post* form of control, were also strengthened, conferring data subjects on-going monitoring powers to keep track of their data once the processing is already in progress. The data protection reform has only further consolidated this expansive tendency. Existing rights have been reinforced; their meaning adjusted and clarified to the new digital reality (e.g., the right to be forgotten or not to be subject to automated decision-making processes) and new right emerged in the GDPR catalogue (right to data portability). The approach of national and EU legislators towards individual participation and control was never drastically revisited and its foundation remained the same throughout the decades, although slightly adapted and contextualized.

OTHER FORMS OF "CONTROL" – Beside "participatory" control mechanisms, key enablers of the "user control" ideal, data protection laws have always included the provision of more "institutional" control mechanisms that relied primarily on the supervisory actions of third-party public independent entities (supervisory authorities). Since its early phases, the establishment of institutional structures, with oversight and enforcement tasks, was deemed an essential condition to ensure a generalized monitoring mechanism on the processing of personal data and safeguard the overall compliance with data protection rules in the interest of the collectivity. Tasks and powers included both certain anticipatory mechanisms of control (e.g., licensing

schemes; prior-authorization and prior-consultation procedures) and *ex-post* measures, manifested in the exercise of investigative and corrective powers. While old licensing schemes and prior-authorization procedures were gradually downsized and simplified, in an attempt to rationalize existing processes and keep up with the mounting datafication of society, this cutback was generally compensated by an enhancement of the supervisory powers of data protection authorities. In any case, these forms of institutional control have clearly a broader scope than mere individual participatory control mechanisms, as they do not only help to protect individual interests, but are directed at safeguarding more generally the interests of the collectivity.

7 A brief hint to European case-law: does individual control over personal data emerge as a defining feature in CJEU decisions?

The analysis of the case-law of the European Court of Justice (the "Court"), in its quality of highest authoritative interpret of EU law[490], provides valuable insights into the interpretation and application of EU legal norms and fundamental rights. This has been particularly the case in developing areas, such as digital privacy and data protection, where the Court has been actively engaged in the past twenty years, showing creativity in the exercise of its judicial powers and consolidating its nearly-constitutional function of ultimate guardian of European fundamental rights.

Since the early 2000s, the Court has been challenged with issues concerning the processing of personal data and has repeatedly delivered important decisions that helped strengthening the role of the right to data protection in the EU landscape vis-à-vis other fundamental rights. Significant in this sense have been the cases that required the Court to reconcile data protection with other rights and interests, such as freedom of information[491]; freedom of expression[492]; intellectual property rights[493]; security interests[494] and the transparency obligations of EU Institutions[495], which have revealed

[490] Alec Stone Sweet, 'The European Court of Justice and the Judicialization of EU Governance' (2010) 5 Living Reviews in European Governance 15 <http://europeangovernance-livingreviews.org/Articles/lreg-2010-2/> accessed 19 June 2021.
[491] Case C-615/13 P, ClientEarth and PAN Europe v EFSA [2010] ECLI:EU:C:2015:489; Case C-553/07, Rijkeboer [2009] ECLI:EU:C:2009:293; C-28/08P Commission v Bavarian Lager [2010].
[492] *Case C-101/01, Lindqvist* [2003] ECLI:EU:C:2003:596; *Case C-73/07, Satakunnan Markkinapörssi e Satamedia* [2008] ECLI:EU:C:2008:727; *Case C-131/12, Google Spain e Google* [2014] ECLI:EU:C:2014:317.
[493] *Case C-275/06, Promusicae* [2008] ECLI:EU:C:2008:54; *Case C-70/10, Scarlet Extended* [2011] ECLI:EU:C:2011:771; *Case C-461/10, Bonnier Audio e a* [2012] ECLI:EU:C:2012:219.
[494] *Case C-92/09, Volker und Markus Schecke e Eifert* [2010] ECLI:EU:C:2010:662; *Case C-291/12, Schwarz* [2013] ECLI:EU:C:2013:670; *Case C-293/12, Digital Rights Ireland* [2014] ECLI:EU:C:2014:238.)

the Court's protective stance for the right to data protection, raising criticisms over the apparent lack of systematic methodology applied in the balancing exercise and the sometimes unjustified prominence conferred to data protection compared to other rights[496]. This favourable tendency of the Court transpires also in decisions, in which the Court offered its guidance in the interpretation of grounding concepts of EU data protection law, supporting an extensive reading of legal provisions (e.g., regarding the notions of "personal data"[497]; "establishment"; "data processing"[498]; "data controller"[499]) or a very strict one (e.g., "consent"[500]) to maximize the level of protection provided by the law. However, it is in some of the most recent and emblematic decisions (*Digital Rights Ireland*[501], *Google Spain*[502], *Schrems*[503] and *Schrems II*[504]) that the role taken over by the Court as "judge made law" has become increasingly apparent in the data protection field[505]. In recent years, the Court has in fact displayed a marked tendency to a judicial activism that, with the aim to expand the umbrella protection granted by EU law, has resulted in a – controversial – extensive "manipulation" (rather than mere interpretation)[506] of secondary data protection norms in light of the new constitutional parameters constituted by Artt. 7 and Art. 8 of the EU Charter. A judicial activism that has at times taken the form of policy action[507], through which the Court boldly attempted to address issues that the political body was to slow or unwilling to face.

Despite the growing case-law and the valuable interventions of the Court on the subject matter, when it comes to clarify the role that "individual control over personal data" plays

---

[495] *Case C-92/09, Volker und Markus Schecke e Eifert* (n 494).
[496] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 174.
[497] *Case C-582/14, Breyer* [2016] ECLI:EU:C:2016:779; *Case C-434/16, Nowak* [2017] ECLI:EU:C:2017:994.
[498] *Case C-101/01, Lindqvist* (n 492); *Case C-131/12, Google Spain e Google* (n 492); *Case C-25/17, Jehovan todistajat* [2018] ECLI:EU:C:2018:551; *Case C-345/17, Buivids* [2019] ECLI:EU:C:2019:122.
[499] *Case C-25/17, Jehovan todistajat* (n 498); *Case C-40/17, Fashion ID* [2019] ECLI:EU:C:2019:629.
[500] *Case Case C-673/17, Planet49* [2019] ECLI:EU:C:2019:801; *Case C-61/19, Orange Romania* [2020] ECLI:EU:C:2020:901.
[501] *Case C-293/12, Digital Rights Ireland* (n 494).
[502] *Case C-131/12, Google Spain e Google* (n 492).
[503] *Case C-362/14, Schrems* [2015] ECLI:EU:C:2015:650.
[504] *Case C-311/18, Facebook Ireland e Schrems* [2020] ECLI:EU:C:2020:559.)
[505] Oreste Pollicino, 'Interpretazione o Manipolazione? La Corte Di Giustizia Definisce Un Nuovo Diritto Alla Privacy Digitale' (2014) 3 federalismi.it - focus TMT <https://www.federalismi.it/nv14/articolo-documento.cfm?artid=28017>.
[506] ibid; Oreste Pollicino and Marco Bassini, 'La Carta Dei Diritti Fondamentali Dell'Unione Europea Nel Reasoning Dei Giudici Di Lussemburgo' (2015) 4/5 Il diritto dell'informazione e dell'informatica 741.
[507] On the political role of the CJEU see: Finocchiaro, 'La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems' (n 464) 115–116; Pollicino (n 396) 569; Giovanni Sartor and M Viola De Azevedo Cunha, 'Il Caso Google e i Rapporti Regolatori Usa/EU' (2014) 4/5 Diritto dell'informazione e dell'informatica 657 ss.

in data protection law, very little insight can be drawn from the Court's jurisprudence. On the contrary, although both EU doctrine and EU Institutions seems to place great importance on the idea that data protection provides individuals with control over their personal data, in the CJEU case-law there is hardly any reference to this aspect. Two different but complementary observations can be made on this point.

CONCEPTUAL UNCLARITY BETWEEN PRIVACY AND DATA PROTECTION - The first, more general, consideration concerns the meaning and understanding of the right to data protection. The Court has in fact not yet unravelled the conceptual difference between the right to data protection and the right to privacy[508]. The various theories on the foundation of data protection that have emerged in EU doctrine, where it is still argued whether this is a product of the "privacy evolution", a direct spin-off of human dignity or a more modern ramification of personal identity or self-determination, appear to have had no particular influence on the CJEU, which has – perhaps with excessive confidence - constantly conflated the right to privacy and data protection under one single cap. In cases involving the processing of personal data, the Court makes regularly cumulative reference to Articles 7 and 8 of the EU Charter, and, despite proclaiming the autonomy of the two rights, it is unable (or reluctant) to clearly highlight the conceptual independence of the right to the protection of personal data from the classic right to privacy[509]. The discomfort of the Court to define the boundaries and, thereby, the different "essence" of the two formally self-standing rights has substantially curbed any attempt to identify through the case-law the "added value" or "distinctive feature" of data protection[510], by many recognized in the ability of people to exercise a comprehensive control over the circulation of their information.

It is true that, when the Court first started to face cases concerning the processing of personal data, the right to data protection had not yet obtained autonomous recognition in the EU legal framework, which it achieved only with the entry into force of the Treaty of Lisbon, in December 2009, when the EU Charter became binding on all Member States. As emerged from previous paragraphs, before 2009, the right to data protection was neither a well-established principle inferred from common constitutional traditions of

[508] Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology 73, 76; González Fuster (n 59) 234–240.
[509] Pollicino (n 505) 5–6.
[510] Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569.

Member States, nor a right explicitly mentioned in the ECHR, unlike the right to privacy which found its place under Art. 8[511]. The DPD, for long time the key piece in the EU framework of data protection, established a clear link between data protection law and privacy including among its objectives the protection of «the *right to privacy with respect to the processing of personal data*»[512]. At the same time, the European Court of Human Rights, to whose case-law the Court has always shown high deference, has persistently addressed issues regarding the processing of data related to individuals through the lens of the "right to private life", enshrined under Article 8 ECHR[513].

Therefore, before the advent of the EU Charter, it was not too unexpected of the Court to emphasize the link between data protection and the well-established right to privacy, rather than carving out an independent existence for the former right[514]. In *Rundfunkt*[515], where the Court was asked to assess the compatibility of a national law requirement with the DPD, the Court approached the case examining whether there had been an interference with the right to privacy, invoking Article 8(2) ECHR as a yardstick to determine compliance[516], thus subsuming data protection rules under the right to private life established by the ECHR. The same reasoning was upheld in *Satamedia*[517]*,* that required to reconcile data protection law with the right to freedom of expression. The Court grounded its judgment exclusively on the supposed objective of the DPD to protect the right to privacy with respect to personal data, followed by the consideration that the object of Art. 9 DPD (i.e., the "processing of special categories of data") was to «reconcile two fundamental rights: the protection of *privacy* and freedom of expression»[518], thus again treating the DPD as a privacy protection tool. *Promusicae*[519] was the first decision, before the EU Charter became binding, to hint at the existence of a fundamental right «that guarantees protection of personal data»[520] (although the sentence was followed by the confusing wording «hence of private life») and to affirm that Article 8 of the EU Charter «expressly proclaims the *right to protection of personal*

[511] ibid 574.
[512] Art. 1 of the DPD.
[513] Fuster and Gellert (n 508) 79.
[514] Lynskey, 'DECONSTRUCTING DATA PROTECTION' (n 510) 574.
[515] *Case C-465/00, Österreichischer Rundfunk e a* [2003] ECLI:EU:C:2003:294.
[516] ibid par. 72.
[517] *Case C-73/07, Satakunnan Markkinapörssi e Satamedia* (n 492).
[518] ibid par. 54.
[519] *Case C-275/06, Promusicae* (n 493).
[520] ibid par. 64.

data»[521]. The ground breaking assertion was however immediately downsized by the subsequent conclusion of the Court that claimed the case required to reconcile the protection of different fundamental rights namely the right to respect for private life, on the one hand, and to protection of property and to an effective remedy on the other. In a similar fashion, in May 2009, the Court pronounced the *Rijkeboer*[522] judgment where it «straightforwardly asserted»[523] that the purpose of the DPD was to protect the privacy of individuals[524].

The binding force acquired by the EU Charter could have provided the CJEU with the necessary legal instruments to elaborate on the content and meaning of an independent right to data protection, however, it was noted, the Court did not size this as an opportunity «to expound a new vision for the right to data protection»[525]. In the first cases after the entry into force of the EU Charter (e.g., *Volker*[526]*, Deutsche Telekom*[527]*, SABAM*[528]) references to Article 8 of the EU Charter and the right to data protection became more frequent, resulting in a change of vision regarding the objective of the DPD, that was now directed to «ensure in the Member States the observance of the right to protection of personal data»[529]. But it also sparked ambiguous allusions to a hybrid «*right to respect for private life with regard to the processing of personal data*»[530]. The definition of the two rights remains fuzzy, their close connection, according to the Court, is still indisputably strong.

The Court's approach, that formally affirms a distinction between the right to data protection and right to privacy but dodges the explanation of their conceptual difference, is reiterated up to the most recent rulings. This emerges in *Google Spain*[531]*,* the notorious decision in which the Court first recognized a "right to be forgotten" as a digitally-adapted version of the right to erasure. In this judgment, the right to privacy and to data protection are recognized as separate rights but are then treated always in conjunction to determine whether the concerned processing activity was compliant with

[521] ibid par. 65.
[522] *Rijkeboer* (n 491).
[523] Fuster and Gellert (n 508) 76.
[524] *Rijkeboer* (n 491) paras 46–47.
[525] Lynskey, 'DECONSTRUCTING DATA PROTECTION' (n 510) 579.
[526] *Case C-92/09, Volker und Markus Schecke e Eifert* (n 494).
[527] *Case C-543/09, Deutsche Telekom* [2011] ECLI:EU:C:2011:279.
[528] *Case C-70/10, Scarlet Extended* (n 493).
[529] *Case C-543/09, Deutsche Telekom* (n 527) par. 50.
[530] *Case C-92/09, Volker und Markus Schecke e Eifert* (n 499); v. Fuster and Gellert (n 513) 77.
[531] *Case C-131/12, Google Spain e Google* (n 492).

the DPD, making it difficult to determine when the reasoning is based on the one or the other. *Digital Rights Ireland*[532] is one of the few rulings in which the Court investigated separately the essence of the right to privacy (Art. 7 of the EU Charter) and the right to data protection (Art. 8 of the EU Charter) to assess whether the adoption of the Data Retention Directive [533] had given rise to an unlawful interference with the said rights. The Court concludes that because the Data Retention Directive required providers to respect «certain principles of data protection and data security», which according to the Court materialize into the implementation of «*appropriate technical and organisational measures*»[534], the retention of data was not such to adversely affect the "essence" of the fundamental right to the protection of personal. Therefore, an important step in reinforcing the difference between the right to privacy and data protection, but a very poor result in a proper conceptualization of the right data protection whose essence is substantially associate to the respect of technical requirements. Also, "control over personal data" is not remotely included in the reasoning of the Court. In another influential judgment that led to the annulment of the EU-US Safe Harbour Agreement[535], the *Schrems* decision[536], the Court affirmed the «importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof»[537] and it looked at Art. 8(3) of the Charter to sustain that the establishment of an independent supervisory authority is «an essential component of the protection of individuals with regard the processing of their data»[538]. However, the court then muddied the water asserting that it is the task of national authorities to «ensure a fair balance between, on the one hand, observance of the *fundamental right to privacy* and, on the other hand, the interests requiring free movement of personal data»[539]. In

[532] *Case C-293/12, Digital Rights Ireland* (n 494).
[533] ibid par. 40.
[534] ibid.
[535] The EU-U.S. Safe Harbor Agreement was a framework of rules that regulated the transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. The Agreement was the main anchor of the "adequacy decision" adopted by the EU Commission, on the basis of Art. 46 of the DPD, that allowed the transfer of EU citizens data to the U.S. The decision, and as a consequence the agreement, were declared invalid in 2015, with the *Schrems* decision, due to a lack of adequate safeguards to ensure protection. The Safe Harbor was later replaced by the EU–US Privacy Shield, a new agreement negotiated with the EU Commission, which however was also declared invalid by the CJEU on 16 July 2020.
[536] *Case C-362/14, Schrems* (n 503).
[537] ibid par. 39.
[538] ibid par. 41.
[539] ibid par. 42.

subsequent judgments, like *Weltimmo*[540] and *Buivids*[541], the Court seems to move even backwards, with affirmations such as that the *right to privacy* of natural persons is laid down in Directive 95/46[542] or that exemptions and derogation in Art. 9 of the DPD must be applied only where they are necessary in order to reconcile two fundamental rights, namely «*the right to privacy* and the right to freedom of expression»[543].

Something may now change with decisions starting to take into consideration Regulation (EU) 2016/679. In *Google*[544]*,* for example, the Court has expressly recognized that the objective of both the GDPR and the DPD is to guarantee the right to the protection of personal data, thus focusing on the latter rather than mixing it up with the right to privacy as in previous decisions. However, the right to privacy remains a big part of the decision and the balancing between conflicting rights sees privacy and data protection always coupled together on the same side of the balance.

The hesitancy of the Court of Justice to dig deeper into the understanding of the two neighbouring rights leaves us with no valuable insights on the conceptualization of the right to data protection, and in particular whether "control over personal data" may be considered the "added value" that characterizes the essence of this right[545].

GENERAL LACK OF MENTION OF "CONTROL OVER PERSONAL DATA" – Even without delving into the intricacies of the privacy-data protection debate, in the reasoning of the Court there is not reference to a broad principle of "individual control over personal data". A number of decisions of the Court have specifically dealt with issues concerning legal instruments that we have previously placed under the "control" principle, such as cases regarding the application of subjective rights or the data subject's consent. Yet, in none of these situations has the Court made an express allusion to this overarching right of individuals to participate, influence and control.

In *Google Spain*, as mentioned above, the Court recognized a "new" individual right of data subjects to require the operator of a search engine to remove, from the list of results displayed following a search made on the basis of the data subject's name, links to web pages published lawfully by third parties ("de-referencing"), on the ground that

[540] *Case C-230/14, Weltimmo* [2015] ECLI:EU:C:2015:639.
[541] *Case C-345/17, Buivids* (n 498).
[542] *Case C-230/14, Weltimmo* (n 540) 53.
[543] *Case C-345/17, Buivids* (n 498) par. 63.
[544] *Case C-507/17, Google (Territorial scope of de-referencing)* [2019] ECLI:EU:C:2019:772.
[545] Lynskey, 'DECONSTRUCTING DATA PROTECTION' (n 510).

he wishes to be forgotten. The Court reached this conclusion employing an extensive interpretation of the individual rights existing under the DPD (right to erasure and to object) and recognizing that the principles of protection laid down in the DPD are reflected in the rights conferred to individuals[546]. It may thus be affirmed that the Court does indirectly refer and support the idea of empowering individuals through the exercise of their individual rights, which entail a form of control over the processing of their information, not only at the moment of first collection but during the course of the data processing. However, no general statement in this regard is ever endorsed. On the contrary, in the only paragraph in *Google Spain* where the Court mentions the exercise of "control over personal data"[547], the latter expression is employed to differentiate the roles of "data controller" and "data processors", thus focusing on the actors that actively process personal data, rather than on the subjects concerned.

In cases concerning the scope of the right to access to personal data, (e.g. *Rijkeboer*[548]*, YS*[549]), the Court affirmed that «the protection of the fundamental right to respect for private life *[protection of personal data]* means, *inter alia*, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner»[550] and that «in order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed»[551]. These decisions also recognize that the right to access is a necessary pre-condition to enable the data subject to exercise other subjective rights, like rectification, erasure or blocking[552]. The same approach is adopted also in the *Bara and others*[553] case, where the right to information of data subject is identified as the pre-requisite for an effective exercise of all the other rights[554]. In this sense, the Court does certainly acknowledge the relevance of individual rights and the practical purpose that they are designed to achieve, namely providing individuals with monitoring powers.

[546] *Case C-131/12, Google Spain e Google* (n 492) par. 67.
[547] ibid par. 34. In particular, according to the Court, the operator of a search engine could not be excluded from the definition of "controller" on the ground that it did not exercise control over the personal data published on the web pages of third parties, given that the activity of a search engines pursued its own and distinct processing purposes, in relation to which the provider operated in its capacity of controller.
[548] *Rijkeboer* (n 491).
[549] *Case C-141/12, YS e a* [2014] ECLI:EU:C:2014:2081.
[550] ibid par. 44.
[551] *Rijkeboer* (n 491) par. 49.
[552] *Case C-141/12, YS e a.* (n 549) par. 44.
[553] *Case C-201/14, Bara e a* [2015] ECLI:EU:C:2015:638.
[554] ibid 33–34.

However, this concept is never advocated nor mentioned explicitly. No additional support can be found in decisions dealing with the data subjects' informed consent, one of instruments typically identified as representations of the subject's ability to control the circulation of his data and individual self-determination. *Planet 49*[555] and *Orange Romania*[556], two of the most recent rulings on the matter, are indeed valuable case-law to strengthen and clarify the characteristic of consent as required by the GDPR, but do not go any further than that.

Some scholars[557] sustain that the Court, albeit indirectly, does in fact support the need for individuals to have legal remedies to exercise their right to control over their personal data, which is the essence of the right to data protection itself. However, the extent to which the Court actually endorses this idea in practice as a general underlying principle of data protection law, that may be applied regardless of a strict compliance with the closed list of individual rights and law requirements, is far from clear.

8 Conclusions

In this First Chapter an attempt was made to investigate the meaning and evolution of the concept of "individual control over personal data" within the EU data protection framework.

It has been observed that the idea of individuals having a right to control did not originate with the first laws regulating the processing of data. It came afterwards, stemming from a right-based and individual-centric conception of data protection. Despite the never settled debate on the fundamental right's roots of data protection, as a direct by-product of human dignity, individual autonomy or privacy, and the lack of clarity from EU case-law on the scope and objectives of this new right, the different values that have been attached to the modern understanding of data protection have been substantiated in the affirmation of a proactive position of data subjects in the management of their personal data. The control individuals exercise on data that relates to them, their preferences, behaviours, characteristics, as "bits" or portions of their identity, becomes the instrument to safeguard the person as a whole, giving voice to his self-determination, autonomy of choice and personal identity. The idea of data subjects

[555] *Case Case C-673/17, Planet49* (n 500).
[556] *Case C-61/19, Orange Romania* (n 500).
[557] See on *Schrems,* Finocchiaro, 'La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems' (n 464) 120.

being in “control”, although never fully acknowledged at jurisprudential level, has grown as an underlying constituent of the right to data protection.

Contrary to the international framework, where a principle of “individual participation” has found express mention, the EU data protection framework has not introduced it in such clear and unitary terms. Data subjects’ empowerment has materialized in the progressive strengthening of the group of subjective rights that, taken together, should potentially provide individuals with the means to decide, manage and control the use and circulation of their information. In particular, rules on consent and information rights, along with other subjective rights (such as the right to access, to data portability, and not to be subjected to solely automated decision-making processes) have been identified as the main legal tools available to data subjects to exercise their control functions.

CHAPTER II – The shortcomings of individual control

1 Introduction

The Second Chapter focuses on the major shortcomings that undermine the idea for individuals to exercise effective control over the circulation of their personal data, whose worsening goes hand in hand with the ongoing datafication of our society.

A survey conducted by the European Commission in 2015 showed that eight out of ten EU citizens felt they did not have control over their data[558]. Only 15% of people felt they had complete control over their information, while half (50%) said they had partial control, and nearly a third (31%) felt that they had no control at all. These numbers have remained worryingly stable even after the GDPR adoption[559]. This circumstance confirms that the hopes that the data protection reform could convincingly re-empower data subjects have not been fulfilled, given the little improvements registered in the ability and perception of citizens to have better control over their data.

The feasibility of individuals to exercise effective control over data processing is facing an increasing number of both older and more recent criticisms that challenge the effectiveness of existing control mechanisms provided under EU law, especially when contextualized in a developing technological scenario, such as the modern society.

In light of this background, this chapter aims at exploring the factors that are contributing to the inefficiency of current individual control mechanisms offered by the EU data protection framework. They can be divided into three main categories: (i) "cognitive", when they refer to the human capabilities of understanding, reasoning and taking decisions; (ii) "systemic", when they relate to exogenous causes connected to technological and structural changes in our society; and (iii) "legal", when the enforcement fallacies depend on unclear legal interpretation and other practical complications.

---

[558] European Commission, Directorate-General for Justice and Consumers, and TNS Opinion & Social, *Special Eurobarometer 431 "Data Protection" Report* (2015) 9 <http://dx.publications.europa.eu/10.2838/552336> accessed 8 June 2021. According to the socio-demographic data, young people and people with a higher level of education are more likely to feel that they have control over their personal information.

[559] European Commission and others, *Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report* (2019) 34 <https://data.europa.eu/doi/10.2838/579882> accessed 8 June 2021. According to the 2019 report, just 14% of respondents felt they had complete control; just over half (51%) felt they had partial control over their information, while 30% felt they have no control at all.

Such categorization provides an overview of the most common variables that affect individuals' ability to exercise their subjective rights to control the circulation of their personal data. However, these factors should not be understood as compartmentalized and independent, since the effects produced by one of these components often affect and emphasize the effects of the others.

2 Cognitive factors

Privacy[560] issues related to the limited cognitive abilities of human beings have long been addressed by legal and social science literature. Scholars have primarily focused on the model of "notice and consent", which is considered one of the pillars of the data protection framework in terms of data subjects' empowerment. Years after its first implementation in the EU framework and despite the improvements introduced by the GDPR, individuals remain poorly informed and mostly unaware of what they are consenting to. The basic argumentation that comes across different works to explain the flaws of this current framework criticizes that the system is benchmarked on an unrealistic model of human being, close to the "rational agent" of classic economics. Evidence, however, has proven that humans are far from rational. Average people have knowledge boundaries, are emotion-driven and often context-influenced. These inherent limitations determine a "short-circuit" especially when information rights and data subject's consent comes into play. Such case scenarios are dealt with separately hereinafter.

2.1 Information overload

2.1.1 Transparency obligations

Transparency is a grounding and characteristic principle of data protection law. It has generally been conceived as a logical extension of the requirement that processing should be performed fairly and lawfully[561]. Codified only in terms of "information obligation" in the DPD (Art. 10 and 11), the GDPR has raised transparency as a general data protection principle, placing it beside the "lawfulness" and "fairness" requirements of processing under Art. 5. The most practical manifestation of this principle remains

[560] Since many contributions and authors use the term "privacy" according to a modern and evolved understanding to refer to what should be more correctly identified as "data protection", the following paragraphs will also employ the term "privacy" in its broadest and modern conception as a synonym for "data protection".

[561] Bygrave (n 14). Brendan Van Alsenoy, Eleni Kosta and Jos Dumortier, 'Privacy Notices versus Informational Self-Determination: Minding the Gap' (2014) 28 International Review of Law, Computers & Technology 185, 186..

that of Articles 13 and 14 GDPR, that require controllers to provide data subjects, at a specific time, a list of information on the data processing[562].

Despite being often coupled with the requirement of consent, transparency has a much broader scope than ensuring that individuals make *informed* (thus theoretically conscious) choices. Adoption of consent as a legal basis, in fact, is only a possibility for the controller, when none of the other five legal grounds (listed under Art. 6 GDPR) applies[563]; whereas the provision of notice is a mandatory requirement that applies under all circumstances, regardless of the chosen legal ground[564]. The principle of transparency essentially emphasizes the "relational" dimension between controllers and data subjects, which is a necessary component of any data processing activity[565]. The rationale behind such principle is that even if a person does not have a say in the processing, he should at least be put "on notice", thus be aware, when his personal data are being processed[566]. In this sense, information requirements are seen as an important tool to remedy information asymmetries between controllers and data subjects on the knowledge acquired regarding the data processing[567]. On the other hand, notices also have the essential function to trigger the control activity of data subjects and make it possible for them to further inquire into the processing activities in which their personal data are involved[568].

Given the above, information imbalances do not only jeopardize the provision of an *informed* consent, but they are also detrimental to the *effective exercise* of other subjective rights (e.g., access, rectification, objection), since in the absence of accurate information data subjects are not able to scrutinize the processing and do not have the means to decide whether to submit a request[569]. Clearly, disclosure obligations may also have effects that go beyond the realization of individual control. They can spur

[562] See in Chapter I, par. 5.3.2.
[563] Refer to art. 6 of the GDPR that lists the six legal basis that legitimize a processing of personal data, among which also the consent of the data subject.
[564] Articles 13 and 14 of the GDPR contain only a few exceptions to the provision of a privacy notice, like the fact that the subject is already informed or that the provision of such information proves impossible or would involve a disproportionate effort.
[565] Marco Dell'Utri, 'Principi Generali e Condizioni Di Liceità Del Trattamento Dei Dati Personali' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (G Giappichelli editore 2019) 199.
[566] Van Alsenoy, Kosta and Dumortier (n 561) 186.
[567] Rouvroy and Poullet (n 48).
[568] Salvatore Mazzamuto, 'Il Principio Del Consenso e Il Potere Della Revoca' in Rocco Panetta (ed), *Libera circolazione e protezione dei dati personali* (Giuffrè 2006) 1004.
[569] Dell'Utri (n 423) 200; Van Alsenoy, Kosta and Dumortier (n 561) 186.

companies to self-examine and improve internal policies[570] and may be helpful to enforce controllers' accountability, providing reference documentation through which data processing activities may be subject to *ex post* scrutiny[571]. In any case, their primary beneficiaries remain data subjects.

2.1.2 Issues: engagement and understandability

Despite the multipurpose function of transparency requirements, the assumption that information notices are efficient instruments to restore data subjects' empowerment clashes with the dynamics of day-to-day reality. A mounting body of literature[572], leaded by some insightful works in the behavioural economics field, has highlighted the inability of notice mechanisms to have any significant influence on people's level of awareness. The two major lines of criticism raised by scholars concern the lack of people's engagement in privacy matters, on one side, and the issue of comprehensible privacy notices, on the other.

ENGAGEMENT – The first objection addresses a commonly discussed trait of privacy notices: people simply do not read them on a regular (or even occasional) basis[573]. The "skim over without reading" is a widespread practice and does not affect only privacy notices, but more generally most of contractual terms and conditions, especially when provided in the online environment[574]. Inevitably, the extent to which individuals are exposed to privacy notices, compared to other contractual forms, intensifies a feeling of "notice fatigue"[575] that demotivates people to pay attention to privacy information even more.

Along with excessive exposure, the predominant reason to explain such low levels of engagement is that privacy policies are too long to read[576], which result in a "information

[570] Ryan Calo, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2012) 87 Notre Dame Law Review 1051, 1052.
[571] Van Alsenoy, Kosta and Dumortier (n 561) 187.
[572] Please refer to the authors mentioned in the following notes.
[573] Solove (n 2) 1883; Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution* (Cham: Springer International Publishing 2018) 115–116.
[574] René Arnold, Annette Hillebrand, and Martin Waldburger, 'Personal Data and Privacy Final Report, Studi for Ofcom' (WIK-Consult 2015) 22–24; Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1884.
[575] Van Alsenoy, Kosta and Dumortier (n 561) 189.
[576] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1885; Frederik Zuiderveen Borgeswius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security & Privacy 103, 105–106.; also Custers et al. found that the most common reason for not reading privacy policies among users of social network sites is that they are too long (55.7% of respondents), Bart Custers, Simone van der Hof and Bart Schermer, 'Privacy Expectations of Social Media Users: The Role of

overload"[577] that, added to short attention spans, easily discourages even the most willing individual. According to some early studies[578], reading the privacy policies that a person runs into during his browsing activity would take several weeks, which clearly exceeds the time expected to be reasonably invested by any person in reading information forms during the surfing activity[579]. This is not only a matter of scale and length of information policies *per se*. Another relevant observation in the context of online activities is that in many instances users spend on the visited webpages only a few moments or minutes, which further reduces their incentive to read privacy policies[580] considering that the time necessary to read such policies would often exceed the time spent on the actual website.

As previously mentioned, the underlying issue is that these information practices are shaped around a false model of human capacity based on the idea of rational individuals with limitless attention capacity (and time)[581]. But in a world with limited time resources that need to be allocated in an efficient way, reading privacy notices is perceived by most as either bearing too much costs or too little benefits[582]. Put it bluntly: people, understandably, deem their time not worth spending on reading endless lists of information all day long[583].

After the adoption of the GDPR, things are apparently slightly better, with more people saying they skim over privacy statements and being at least sometimes informed about the conditions under which their data are collected and may be used further[584].

Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users' (2014) 6 Policy & Internet 268, 291 <http://doi.wiley.com/10.1002/1944-2866.POI366> accessed 8 June 2021.

[577] Bergemann (n 573) 115–116.

[578]Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 J. L. & POL'Y FOR INFO. SOC'Y 543.. The study refers to data from 2007, hence these results may underestimate the level of disengagement in reading privacy policies, considering the increase in the use of Internet and exposure to privacy policies.

[579] Bergemann (n 573) 115–116; René Arnold, Annette Hillebrand, and Martin Waldburger (n 574) 20–25.

[580] René Arnold, Annette Hillebrand, and Martin Waldburger (n 574) 20–25; Tony Haile, 'What You Think You Know About the Web Is Wrong' (*Time*, 9 March 2014) <https://time.com/12933/what-you-think-you-know-about-the-web-is-wrong/> accessed 8 June 2021.

[581] Calo (n 570) 1054.

[582] For example according to McDonald and Cranor the time that website visitors need to invest in reading privacy policies is, in and of itself, a form of payment, which could justify why people are not reading long privacy policies, McDonald and Cranor (n 578); Van Alsenoy, Kosta and Dumortier (n 561) 32.

[583] To prove the absolute indifference to privacy policies, Borgeswius illustrates the case of a UK website that obtained the soul of 7500 people, because they did not opted out from the website's terms and conditions that granted the webstore «a non-transferable option to claim, for now and forever more, your immortal soul», Borgeswius (n 576) 105–106.

[584] In the 2019 Eurobarometer survey, 60% of respondents said they read privacy statements "at least partially", with 57% of respondents declaring they were in any case "at least sometimes" informed about the processing of their data. However, out of these, just over one in five (22%) said they were always

However, still only one out of five persons is *always* informed about processing operations concerning her, whereas the length of privacy statements remains by far the most common reason users are discouraged from reading them in full[585].

UNDERSTANDABILITY – For the sake of discussion, let's imagine a person with no time-constraint and considerable will power, who decides to invest his days in reading every privacy notice he encounters. Would he understand what he is reading? According to many, no. Poor comprehension of privacy notices can be attributed to a number of factors.

First, data processing operations have substantially grown in complexity and technicality, thus have become more difficult to understand, often even for specialists of the sector, let alone average users[586]. The same difficulty is experienced in the assessment of the possible consequences and risks stemming from the disclosure of personal data. The different purposes and multiple contexts in which personal data may be used and further exchanged, even years after their original collection, makes the perception of the negative, but also positive, consequences triggered by the first data disclosure very nebulous. They are often too abstract or remote to be fully assessed[587]. These limitations in human understanding give rise to a fundamental dilemma in notice drafting. Making easier, thus more accessible, privacy statements does not fully inform people about the processing and the related and envisaged consequence, because less granular information necessarily implies less information[588]. However, if information on the data processing is provided in sufficient detail, the explanation becomes too complex to be anything meaningful for the user[589].

---

informed, while 35% say they were sometimes informed. A further 21% say they are rarely informed, while 13% say they are never informed.
European Commission and others (n 559) 42–47.

[585] According to the 2019 Eurobarometer, 66% of respondents affirmed that privacy statements are too long to read. ibid 51 ff.

[586] Bergemann (n 573) 116; Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Helen Nissenbaum and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 59; Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law & Security Review 643, 651.

[587] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 188.

[588] Bart-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 252.

[589] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1885.

Secondly, often the language of privacy statements is at the same time very legalistic, characterized by formal and technical jargon[590], and over-generic[591]. The reasons for this linguistic choice are varied: from the desire to protect the controller as much as possible, to avoiding detailed explanations that would constrain the organization in its future uses and abuse of copy-paste habit[592]. The consequence is, however, that understanding a privacy notice requires high reading competences, which ditches any accessibility and attractiveness for average end-users. This circumstance has not changed with the GDPR. Surveys show that unclarity of privacy statements and difficulties in understanding their language rank high in the reasons driving individuals not to read them[593].

Finally, exacerbating the difficulties of providing comprehensible privacy policies is also poor general privacy literacy and false convictions that users have on how their privacy is protected[594]. The data protection reform has helped in promoting a privacy culture and in increasing people awareness on the existence of the GDPR, and data protection in general[595]. Nevertheless, evidence suggests that people still lack sufficient knowledge about the matter to fully exercise the rights granted by the GDPR[596]. Further, people seem to maintain a naïf approach on privacy and frequently believe that it is sufficient that a privacy banner is displayed on a website to prove its compliance with law, therefore assuming their data is fully protected[597].

2.2 The limits of consent

2.2.1 Data subject's consent

Consent is one of the six legal basis that, when rightfully obtained, allows controllers to legitimately process personal data. The GDPR, together with national DPAs' guidelines, has seek to reduce the improper overuse of consent as a ground for processing,

[590] Bergemann (n 573) 116; Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1884.
[591] Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (n 586) 651; Van Alsenoy, Kosta and Dumortier (n 561) 189..
[592] Van Alsenoy, Kosta and Dumortier (n 561) 189.
[593] European Commission and others (n 5) 51 ff.
[594] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1886.
[595] In 2019, 67% of respondents had heard about the GDPR. European Commission and others (n 5) 20 ff.
[596] According to the 2019 Special Eurobarometer, 63% of users do not know what the GDPR is about or have never heard of it. ibid.
[597] 17% of respondents in 2019 said it was enough for them to see that the website had a privacy policy and 15% believed the law would protect them in any case. European Commission and others (n 559).

toughening the conditions needed to meet it[598] and giving prominence to the other existing grounds[599]. Nonetheless, the appeal of consent remains strong. Whether because it is considered the most flexible and safe justification, the maximum expression of individual autonomy or because it remains an express condition required by law[600], companies and organizations still make great recourse to consent, especially in the context of online activities.

2.2.2 Issues: bounded-rationality and manipulations

This heavy reliance on consent has been followed by intense criticisms questioning the capability of people to make conscious decisions when it comes to choosing whether or not to disclose their personal data. Despite surveys often report a high level of interest and care for privacy matters[601], evidence shows that, when faced with a choice, people turn easily over their data for small benefits[602]. This tendency proves a worrying disconnection between what people say to care and what people do in practice.

BOUNDED-RATIONALITY - The issue can partly be ascribed to the information gaps cited in the previous paragraph, but also to a "skewed" decision making process which is typical of human beings[603]. Like the transparency scheme, the GDPR consent mechanism is built on a faulty model of the "rational agent". In reality, people's behaviors are rarely inspired by pure rationality, rather they are influenced by a number of cognitive impediments and biases[604]. Individuals' "bounded rationality" limits their ability to process and apply relevant information to complex situations[605]. They often rely on heuristics, in other words mental short-cuts, and other approximate strategies to

[598] Art. 4(11) and Art. 7 of the GDPR. See Chapter I, par. 5.3.2.
[599] Art. 6 of the GDPR lists other five legal basis: performance of a contract; compliance with a legal obligation; protect vital interests; performance of a task carried out in the public interest; legitimate interest of the controller or a third party.
[600] Directive 58/2002/EC (e-privacy Directive) requires that the data controller obtains the consent of the concerned subject for a number of operations, such as using profiling cookies, collecting location or traffic data. See Chapter I, par. 5.3.
[601] Lucilla Gatt, Roberto Montanari and Ilaria Amelia Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 48 Politica del diritto 363; Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1886; Chris Hoofnagle and others, 'How Different Are Young Adults From Older Adults When It Comes to Information Privacy Attitudes & Policies?' [2010] Departmental Papers (ASC) <https://repository.upenn.edu/asc_papers/523>.
[602] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1886; Alessandro Acquisti and Jens Grossklags, 'Privacy and Rationality' in Katherine J Strandburg and Daniela Stan Raicu (eds), *Privacy and Technologies of Identity* (Springer-Verlag 2006).
[603] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1886.
[604] Bergemann (n 573) 116.
[605] Term coined by Aquisti and Grosslaks, Acquisti and Grossklags (n 602) 25–26. See also Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1886; Borgeswius (n 576) 106.

take a decision[606]. Individuals usually assess the risks linked to a data disclosure based on examples or events that can quickly retrieve to their mind (e.g., news of people being scammed for providing their data to a certain provider or the bad reputation of a certain company). Following this timesaving approach, however, unfamiliar dangers are considered less probable than familiar ones[607], which deceives data subjects in believing that something will not happen based on very flimsy clues. At the same time, tangible privacy harms are often cumulative in nature[608], namely they may emerge as the downstream result of the different decisions on data disclosure and uses that an individual has made over time. This makes consequences hardly perceivable by individuals when they have to make isolated decision, far away in time[609].

The cost-benefit assessment is further aggravated by other typically human distortions, such as "present myopia" (i.e., the tendency to choose for short term gains and disregard future disadvantages)[610] and "optimism bias" (i.e., propensity to disregard the probability of a negative event occurring)[611], which make assessing the harms of data sharing with respect to long-term consequences very challenging and contribute to further skew individuals' decision making.

MANIPULATIONS - The context and the way privacy choices are presented can fundamentally affect individuals' privacy preferences. Controllers can exploit human biases to activate or suppress privacy concerns, thus influencing data subjects' behaviour and making their privacy preferences malleable[612]. These mental tricks are more widely known as "dark patterns"[613], namely layout and design choices that can

[606] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Rev and expanded ed, Penguin Books 2009) 9. Among different studies conducted in this field, see e.g., S Shyam Sundar and others, 'Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key?', *CHI '13 Extended Abstracts on Human Factors in Computing Systems* (Association for Computing Machinery 2013).
[607] Referred to as "availability heuristics", a mental short-cut that relies on information and examples that comes to mind quickly. Thaler and Sunstein (n 606) 25.
[608] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1891.
[609] ibid.
[610] Alessandro Acquisti and others, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50 ACM Computing Surveys 1, 6; Borgeswius (n 576) 106.
[611]Acquisti and others (n 610) 190.
[612] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509 <https://www.science.org/doi/10.1126/science.aaa1465> accessed 20 November 2021.
[613] Acquisti and others (n 610) 25–26; European Data Protection Supervisor, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (19 March 2019); Giovanni Sartor, Francesca Lagioia and Federico Galli, 'Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent' (European Parliament's Committee on Legal Affairs 2021) 46.

manipulate users' behaviour and distort their decision-making process, often inducing to over-share personal data or blindly accept certain processing purposes[614].

Studies demonstrate that people are more inclined to consent to share their data when they have a, real or illusory, feeling of being in control[615]. By increasing the perceived sense of control data subjects experience (e.g., through user-friendly design or reassuring communications), controllers may be able to deceit users into influencing their decision-making process.

Evidence has also shown that people may be deeply influenced by the manner in which the consent form is presented[616]. Due to a *status quo* bias, when people encounter opt-out choices or default privacy settings, few of them take the trouble to make a proactive choice (opting out or changing privacy settings) and most prefer to stay with what is given[617].

Finally, controllers may win the resistance of users unwilling to consent to data practices by relying on the "annoyance effect"[618]. This is when consent requests (e.g., cookie banners and pop-ups) are presented repeatedly and persistently to users until they agree, which they are ultimately forced to do to enjoy the service undisturbed.

In sum, even if people had the time and capability to read and understand privacy notices, their privacy choices remain easily influenced by a variety of non-rational factors, that controller can twist and tailor at their convenience.

2.3 Externalities of individual privacy choices

Privacy self-management[619] assumes that people decide about disclosing personal data based on their subjective costs and benefits. This individualistic focus, however, fails to account for the impacts that individual privacy decisions may have on other individuals and on society at large.

---

[614] For an overview of the types of dark patterns see the list updated in https://www.darkpatterns.org/ .
[615] Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2013) 4 Social Psychological and Personality Science 340, 345.
[616] Van Alsenoy, Kosta and Dumortier (n 6) 190; Calo (n 15) 1054 ff.
[617] Gatt, Montanari and Caggiano (n 46); Solove (n 2) and the studies mentioned there. See also Borgeswius (n 576) 106.
[618] Jacob Leon Kröger, Otto Hans-Martin Lutz and Stefan Ullrich, 'The Myth of Individual Control: Mapping the Limitations of Privacy Self-Management' [2021] SSRN Electronic Journal 5 <https://www.ssrn.com/abstract=3881776>.
[619] As already clarified, the concept of "privacy self-management" has been taken over from Solove's works, which translates into the ability of individuals to control and manage their data, identified by the author essentially in the notice and consent model. Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12).

Several scholars have emphasized the social function of privacy and data protection, arguing they should not be treated as a mere individual interests, at the disposal of individuals' preferences, rather as a collective value, precondition for maintaining meaningful democracy[620].

The connection between privacy and broader societal interests was evident especially in the early data protection legislations[621], adopted as a consequence of the collective fears of governance surveillance and mass collection of citizens' data[622]. The adoption of rules to govern the automated collection and use of citizens' data was more about safeguarding the general values of a democratic society[623] against unlawful interferences from the state, rather than protecting individual interests. Whereas the individual-centric turn of data protection shifted the focus on individual interests, these wide-society goals have remained a fundamental aspect of data protection.

The strict link between privacy and the safeguard of the "quality" of society in general[624] finds confirmation in a number of contributions. Rouvroy and Poullet define privacy and data protection as «social-structural tools for preserving a free and democratic society»[625]. From the analysis of EU data protection laws, Bygrave identifies democracy and pluralism[626] among the primary social concerns pursued by data protection laws[627]. Further, Regan[628] and Schwartz[629] also recognize the function of privacy as serving common, public and collective purposes and bearing an inherent relation to participatory democracy. Mantelero recognizes in the safeguard of equality and prevention of unlawful discriminations; freedom of association and limitation to disproportionate surveillance that main societal benefits of privacy and data protection[630]. Other authors

[620] Van Alsenoy, Kosta and Dumortier (n 561) 190.
[621] B van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307, 324.
[622] See further Chapter I, par. 3.
[623] Mayer-Schönberger (n 67) 223.
[624] Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 Computer Law & Security Review 238.
[625] Rouvroy and Poullet (n 48) 57.
[626] Bygrave (n 14) 151–153.
[627] Bygrave identifies two additional wide-societal concerns addressed by data protection, which are the "rule of law" and "civility".
[628] Priscilla M Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (The Univ of North Carolina Press 2009).
[629] Paul M Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices' [2000] Wisconsin Law Review.
[630] Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 624).

have argued that privacy is a fundamental value to ensure the promotion of creativity and innovation[631].

As asserted by Solove, «privacy self-management does not prevent, redress, or even consider infringements on those social values»[632]. Individuals are in no position to understand and calculate these wider societal benefits and harms. For example, individuals may have an interest in consenting to ad-targeting practices that may ultimately lead to fuel micro-targeting political campaigns that pose a direct threat to electoral freedom and democracy[633]. Similarly, consumers may have an interest to consent that their driving behaviours are tracked to lower their insurance rates, but such data may ultimately lead to the development of an algorithm with discriminatory outcomes on more vulnerable categories[634].

The direct and immediate externalities that individual privacy choices may have on other people have become even more evident in the context of modern profiling techniques, powered by Big Data and advanced software analytics (see further under par. 3.2 *infra*). Technological advances have dramatically increased the possibility of making predictions and inferring information of an individual, from data that have been collected and shared by others[635]. Personal data can in fact be used to build profiles that are applicable to the broader group of people that share certain similar characteristics – such as social conditions, behaviour, psychological traits – with those who originally disclosed those data or, on the contrary, can lead to the exclusion from that group of certain individuals for not sharing such traits, without them having consented to the

---

631 Gordon Hull, 'Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data' (2015) 17 Ethics and Information Technology 89, 93 ff.

632 Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1893.

633 Jacob Leon Kröger, Otto Hans-Martin Lutz and Stefan Ullrich, 'The Myth of Individual Control: Mapping the Limitations of Privacy Self-Management' [2021] SSRN Electronic Journal 7 <https://www.ssrn.com/abstract=3881776> . The impacts of political micro-targeting on election results have been subject to intense scrutiny following the "Cambridge Analytica" scandal (that uncovered the employment of millions of users' data to create targeted political messages and news) that was variously linked to the Trump Campaign for the 2016 U.S. election and the Brexit referendum. Alex Hern, 'Cambridge Analytica: How Did It Turn Clicks into Votes?' *The Guardian* (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 15 October 2021; Carole Cadwalladr, 'Follow the Data: Does a Legal Document Link Brexit Campaigns to US Billionaire?' *The Observer* (14 May 2017) <https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns> accessed 22 December 2021.

634 Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' [2016] SSRN Electronic Journal 36 <http://www.ssrn.com/abstract=2784123>.

635 Rainer Mühlhoff, 'Predictive Privacy: Towards an Applied Ethics of Data Analytics' [2021] Ethics and Information Technology 4 <https://link.springer.com/10.1007/s10676-021-09606-x>.

processing or provided their own data[636]. As a consequence, individuals may be assessed, ranked or subject to certain decisions (with potentially unfair discriminatory and biased outcomes) based on group profiles that they have not contributed to build or that do not represent them fully[637].

Therefore, even assuming that individuals have control and can consciously consent to the processing of their personal data, they are unaware, cannot anticipate and are not able to control how their data will be used on others[638]. This circumstance creates negative collective externalities, stemming from dozens of lawful individual choices (to share their data), that do not only impinge on many others' right to autonomy, identity and self-determination (of not being profiled or being categorized in ways that do not reflect them), but may also contribute to build systems that increase unfair forms of discrimination and social inequalities, with deep societal consequences.

These considerations add a further layer of "myopia" to the individual control model. This form of control serves primarily the achievement of an individualistic sense of privacy, as an expression of personal choices. This is at odds with a scenario in which the impacts of the processing of an individual's personal data transcend the individual sphere and directly affect other people's sense of privacy and broader social values. Individuals are not well-positioned to see this bigger picture, as well as the consequences that certain processing activities may have on groups and society at large.

3 Systemic factors

A number of technological changes that our society has experienced in the last decades have contributed to reduce the ability of data subjects to achieve optimal awareness and control over the processing of their personal data. Technological factors have in fact added new layers of complexity to the data processing context that have worsened existing human rationality limits and have given rise to problems of their own.

---

[636] Sartor, Lagioia and Galli (n 613) 104.
[637] Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 624); Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer Netherlands 2008) 19–20.
[638] Mühlhoff (n 635) 4.

3.1 Data market ecosystem

3.1.1 Too many roosters in the henhouse

Data has undeniably become one of the most precious resources of our time, compared by many, in terms of value and characteristics, to the gold of the 21st century[639], the oil of the digital age[640] , or, more recently, the new water[641]. Data is fueling a new industrial revolution driven by digital data, computation, and automation[642] and is placed at the center of our future knowledge society. It plays an essential role in job creation and societal wealth[643], it drives productivity and resource efficiency and is at the basis of the development of new products, personalization of services and training of sophisticated AI systems[644].

The global frenzy around data has led to the emergence of a data-driven economy, characterized by an ecosystem of different types of market players interacting and collaborating with each other to collect, use, sell and store available information[645]. Clearly, the value of data does not only lie in "personal" data that fall under the special protection regime of the GDPR, but also in "non-personal" data generated by sensors and machines. However, personal data remain a very precious and competitive assets for organizations, that drives business developments by extracting useful insights from the population of consumers and users. In addition, clear boundaries between the definitions of personal and non-personal data are progressively more difficult to trace, given that data generated by sensors (e.g., car sensors) and devices (e.g., mobile

[639] Mike Lynch, 'Data Wars: Unlocking the Information Goldmine - BBC News' *BBC News* (13 April 2012) <https://www.bbc.com/news/business-17682304> accessed 14 June 2021; Brad Peters, 'The Big Data Gold Rush' *New York: Forbes Magazine* (21 June 2012) <https://www.forbes.com/sites/bradpeters/2012/06/21/the-big-data-gold-rush/> accessed 14 June 2021.

[640] Kiran Bhageshpur, 'Council Post: Data Is The New Oil -- And That's A Good Thing' *Forbes* (15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/> accessed 14 June 2021.

[641] StJohn Deakins, 'Data Is The New Water: Seven Reasons Why' *HuffPost UK* (12 October 2017) <https://www.huffingtonpost.co.uk/stjohn-deakins-/data-is-the-new-water-sev_b_18228184.html> accessed 14 June 2021; IDC Infobrief, sponsored by Qlik, 'Data as the New Water: The Importance of Investing in Data and Analytics Pipelines' (2020).

[642] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Thriving Data-Driven Economy' (2014) COM/2014/0442 final 2..

[643] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building A European Data Economy' (2017) COM (2017) 9 final 2.

[644] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' (2020) COM(2020) 66 final 2.

[645] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building A European Data Economy' (n 643) 4.

phones, house devices) can be easily used to identify individuals and that re-identification techniques are swiftly knocking down the defenses erected by anonymization procedures[646]. Therefore, most technologies nowadays involve some kind of processing of personal data, whether we are conscious of it or not.

The number of private and public actors striving to consume and share data is growing at a quick pace, generating complex networks of entities that extract knowledge from multiple sources[647]. The cross-cutting value and competitive advantage that originate from data analysis[648] have not only pushed small and big entities to a data collection rush, but have also created an entirely new market (the so-called "data market") populated by traditional market players, and new businesses specialized in the provision of data-related services.

Although only a small number of Big Tech firms (Apple, Google, Amazon, Facebook) hold a large part of the world's data[649], these big companies act as new data intermediaries that gather around them a thriving ecosystem of data "users" and data producers[650]. Due to their data collection and analysis capacities and the richness of their data catalogue[651], online platforms have reached a unique and privileged position in the data market[652] and are surrounded by a varied number of stakeholders (e.g., smaller platforms, big and small businesses, data brokers, regulatory and other public authorities) that need to exploit online platforms' data power[653]. The types of data access models adopted by these platforms[654] further contribute to define the level of

[646] See *infra* para. 3.2 and 3.3 in this chapter.
[647] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Murray 2013) 124–125; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' (n 644) 2.
[648]Yves-Alexandre De Montjoye, Heike Schweitzer and Jacques Crémer, *Competition Policy for the Digital Era.* (European Commission 2019).
[649] AGCOM, AGCM, Garante per la protezione dei dati personali, 'Indagine Conoscitiva Sui Big Data (Annex 1 Resolution n. 458/19/CONS)' (2019).
[650] Mayer-Schönberger (n 67) 125.
[651] Teresa Rodríguez de las Heras Ballell and others, 'Work Stream on Data: Final Report' (European Commission 2021) 15–17.
[652] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' (n 644) 8; Ballell and others (n 651) 14.
[653] Mayer-Schönberger and Cukier (n 647) 21.
[654] The data sharing models can be classified in: open data model, data monetization model, data marketplace model, exclusive data platform model. See for a detailed overview of different data sharing models, Elizabeth Scaria and others, *Study on Data Sharing between Companies in Europe: Final Report.* (European Commission 2018) 61–64; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and

data mobility (sharing and re-use) and the number of players that can obtain and employ their information, establishing a long and possibly infinite chains of actors. “Data brokers,” namely companies specialized in data harvesting and analysis, are also filling important gaps in the data market, providing businesses with information gathered from multiple sources digested into actionable business insights[655]. Data analyst companies and other data-related suppliers, whose main activity is the production and delivery of digital products, services, and technologies, are also creating a new and flourish sector that is only expected to expand in the next years[656]. In addition, the enormous diversity of sources from which data can be collected (e.g., online, IoT applications) and the necessity to invest in enabling infrastructures for a data-driven economy (e.g., for cloud computing or 5G technologies) are creating space for new players to join the market, like IoT and infrastructure providers[657].

Beside the scale and number of actors in the data market, the re-use of data is another decisive factor that contributes to the intensified dispersion of data across different entities. The value of data lies in fact not only in its use, but (and increasingly more in a big data age), in its re-use[658]. Re-using and sharing data to generate new knowledge is at the basis of the “data value chain” concept[659]. This does not only mean that data originally collected for a specific purpose may be further used by the original collector for different purposes, once enriched, mixed, and supplemented with other data. It also means that several entities may find a single data set useful to perform the most diverse activities. This multipurpose feature of data, combined with the high costs of its collection in the first place, contributes to pump trade mechanisms by which those who

---

the Committee of the Regions. Towards a Common European Data Space.’ (2018) COM(2018) 232 final 5..

655 See Brigid Richmond, ‘A Day in the Life of Data: Removing the Opacity Surrounding the Data Collection, Sharing and Use Environment in Australia’ (Consumer Policy Research Centre 2019) Report 8; Ballell and others (n 651) 18. The key value proposition of data brokers lies in their ability to bring together a combination of sources, as well as superior technical and analytical capacities, innovative tools and approaches. Data brokers use highly advanced technical methods to extract data (scraping or crowdsourcing business user account data) or they buy data from online and offline sources.

656 Mike Glennon and others, *The European Data Market Monitoring Tool. Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories. D2.9 Final Study Report.* (European Commission 2020) 33–35..

657 European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Common European Data Space.’ (n 654) 9–10.

658 European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data’ (n 644) 6.

659 European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building A European Data Economy’ (n 643) 4.

have data are willing to share it, often for a certain price, and those who want data are able to receive organized data sets that they can re-purpose for their activity.

To provide practical examples of this intricate ecosystem of players, the sectors of digital targeted advertising (the so-called "Ad-tech industry") and connected cars offer two good examples. As for digital advertising, the number of companies that have a role in the collection or processing of consumers' personal data, for the distribution of a single online ad banner, may include most (if not all) the following subjects: the targeting company, a social media provider, a marketing service provider, an ad network and ad exchange company, a data management provider (DMPs) and a data analytics company[660]. The network of stakeholders is even more complex in the field of connected vehicles. In this case the ecosystem of entities is not limited to the traditional players of the automotive industry, but is shaped by the emergence of new players that offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping[661]. Further, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators also play an important role with respect to the potential processing of drivers' and passengers' personal data[662].

Increased pressure to intensify the availability of data across stakeholders in the market, encouraging the sharing and re-use of information, is promoted especially by EU Institutions. In a recent Communication that outlines the EU strategy for policy measures and investments to enable the data economy for the coming five years, great emphasis is placed on business-to-business and business-to-government data sharing[663]. The aim is to create a single "European data space", namely «a genuine single market for data, open to data from across the world, where personal as well as non-personal data, including sensitive business data, are secure and businesses also

[660] For an overview of the different actors, see Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (22 June 2010) WP 171 5. See also the European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (13 April 2021) 10.

[661] See Article 29 Data Protection Working Party, 'Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)' (4 October 2017) WP 252; European Data Protection Board, 'Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications' (9 March 2021) 4.

[662] European Data Protection Board, 'Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications' (n 661) 4.

[663] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' (n 644).

have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value»[664]. The action line of the European Commission only reinforces the trend of an expanding data ecosystem that will incorporate additional stakeholders and create increasingly complex networks of data suppliers and data users.

3.1.2 Issues: problem of scale, qualification and lack of real choice

Against this background, characterized by an indefinite chain of actors and intensified secondary-uses, data protection principles are facing rising challenges. The significant impacts of technological and market changes are particularly evident with respect to the ability of data subjects to effectively monitor and keep track of, and in this sense control, the flow of information that they spread in the course of their day-by-day activities, which is substantially compromised.

PROBLEM OF SCALE – The first issue is what Solove would call a "problem of scale"[665]. The populous landscape of data supplier and data user companies makes it almost impossible for individuals to keep track, or even gain knowledge, of the multiple parties that may be directly or indirectly involved in a data processing that concerns them. Even the simplest operation, like the purchase of a product on an e-commerce website, involves in the baseline scenario a multitude of entities ranging from the company owning the website, affiliates of the e-commerce company, the producer of the purchased good, up to various firms that provide the latter with storing, counselling and other administrative services, as well as payment service providers. If marketing and profiling activities are involved, consumer's personal data would travel even further, throughout the web of agencies and providers that populate the Ad-tech sector. Indeed, Art. 13 GDPR requires that privacy notices provided to data subjects contain, beside the identity of the data controller, the indication of the «recipients or categories of recipients of the personal data»[666]. Since it is usually too burdensome for companies to enumerate (and keep up to date) a detailed list of recipients, the requirement is respected most of the time through a list of macro categories of providers, which give individuals a very vague idea of where their personal data is going to end. And even if a full record of the receiving companies were to be displayed or made available, it is uncertain that the detailed list would satisfy the awareness standard that the GDPR requires for data

[664] ibid 4.
[665] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1888.
[666] Article 13(1)(e) of the GDPR.

subjects to be active participants in the data governance. Due to increased data mobility and opaque business practices, whereby data exchanges between companies are not transparently disclosed, the perception of individuals around their data processing is drastically reduced.

DIFFICULT QUALIFICATION - A second set of issues raised by the number of players involved concerns the correct allocation of privacy qualifications ("data controller"[667], "joint controllers"[668] and "data processor [669]) that determine the ultimate responsibility to ensure that data subjects' rights are correctly enforced along the chain of actors involved in a processing operation. The duty is generally assigned to data controllers or joint controllers, since they are the "lead operators" of a data processing; in other words, they are those who decide the how, why and when the data are used. However, the interaction of multiple players makes the assignment increasingly difficult. These roles are not always clear-cut in a market where companies carry out "mixed-processing", both in the quality of processors, for the provision of third-party services (e.g., storage or analysis), and controllers, for the improvement and development of their business activities[670]. In other cases, the relationship between data-user companies is ambiguous due to the different level of involvement that organizations have in the processing of personal data[671] or the difference in their market power[672]. This level of uncertainty jeopardizes the liability structure that the GDPR has set up to allocate clear

[667] Art. 4(7) of the GDPR defines data controller as «the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law». See also European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (7 September 2020) 9.

[668] When more entities share this decision-making power then a joint controllership relationship is established according to Art. 26 of the GDPR. ibid 16 and ff.

[669] Data processors are entities that carry out data processing in the sole interest and following the instruction of a data controller. Art. 4(8) of the GDPR. ibid 24.

[670] For example, the case of Company X that provides promotional advertisement and direct marketing services to Company Y, but uses the customer database of Company Y also to refine its targeting services and develop its business activities. ibid 25.

[671] There was much discussion around the privacy roles of social media platforms and "targeter" companies in the context of targeting social media users. Following the relevant case-law of the CJEU in the cases *Wirtschaftsakademie* (C-210/16), *Jehovah's Witnesses* (C-25/17) and *Fashion ID* (C-40/17), the EDPB qualified both subjects, in most targeting scenarios, as "joint controllers". European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (n 660).

[672] For example, in the case of cloud service providers ("CSPs") the European Data Protection Supervisor (EDPS) has underlined how although CSPs are usually only processors, for many CSPs on the market «the role of the service provider is not always clear. Sometimes CSPs keep a level of control over the processing that exceeds the role of the processor by carrying out operations on personal data that have not been requested by the customer or not leaving the customer enough choice on the processing means or procedures». European Data Protection Supervisor, 'Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies' (16 March 2018)..

responsibilities, thus leaving data subjects confused and without clear points of reference to which they can address their requests.

LACK OF REAL CHOICE – Another often-cited issue of new data-driven business environment is that consumers are rarely offered "real" choices, when asked for their consent to process personal data[673]. Highly standardized privacy policies leave to individuals no room to negotiate with the controller the amount or type of data they would like to share and leaves them with a "take it or leave it" deal[674]. Lack of choice is reinforced by a lack of real alternatives due to the effect of market concentrations that create social and technological lock-ins[675]. As a consequence, to benefit from a certain service, data subjects often have no choice but to consent, given the absence of alternative privacy-friendly options[676]. Both the GDPR and the EDPB have stressed that a "free consent" can never be linked to the provision of a service or product and that data subjects should be able to refuse their consent without having any detriment[677]. Current trends, however, show some opening with respect to the possibility for providers to tie the provision of certain services to the sharing of consumers' personal data as a form of counter-payment, which makes this type of bundled choices ever more dangerous.

3.2 Big data and analytics

3.2.1 My choice is your choice

The term "big data" has different definitions, commonly used to identify data analysis practices which share certain recurrent features in terms of the huge volume of data processed, the variety of data and data sources, and the sophistication of the analysis tools employed[678]. Big data do not only relate to data quantity, complexity, and

[673] Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 160.
[674] Bergemann (n 573) 115; Custers, van der Hof and Schermer (n 576) 160.
[675] Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (n 586) 4–5.
[676] Koops (n 588) 252; Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (n 586) 4–5.
[677] Recitals 42-43 of the GDPR; European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 437) 10–11.
[678] Volume, Variety and Velocity were identified as the traditional features that distinguished "big data" analysis techniques from "small data" analysis procedures in Douglas Laney, '3D Data Management: Controlling Data Volume, Velocity, and Variety | BibSonomy' (META Group 2001) <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. and Mark Beyer and Douglas Laney, 'Report: The Importance of Big Data: A Definition' (Gartner Analysis 2012). For a detailed analysis of these features, see also Antoinette Rouvroy, '"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data' (Bureau Of The

proliferation speed but also to the new software techniques that allow to make use of the immense mass of accumulated data and extract useful knowledge[679]. Essentially, big data represent an empowered form of data mining[680], or in other words, a more powerful version of knowledge discovery in databases. Big data, in fact, improve and upgrade the extraction of hidden information and unexpected correlations where it would have been impossible before.

Big data have boosted the potential of data analytics, hence the analysis of datasets to find trends and patterns based on correlations of data (at the basis of "profiling" and "clustering" models) and have been particularly valuable for *predictive* analytics processes, that make assumptions based on past data to predict future events (for example, to predict the behaviour of a certain individuals or groups)[681]. Another blooming area of data analysis in the age of big data concerns AI machine learning analysis, which brings predictive analysis to a new level of scale, depth and accuracy as it allows machines to autonomously learn and improve their predictions based on past outcomes[682].

The expectation behind these enhanced analysis capabilities is that they may ultimately lead to better and more informed decisions, based on more accurate and personalized insights. Extensive literature has been devoted to review the cross-sectoral applications of big data and highlight their striking benefits in a varied number of areas[683]. Big data

---

Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data 2015) Ets 108 5–8. These initial "three Vs" have in time been complemented with a number of other "Vs" that characterize the big data phenomenon such as: veracity; valence; visualization. AGCOM, AGCM, Garante per la protezione dei dati personali (n 649) 8. According to the general and dynamic definition offered by the McKinsey Global Institute «"Big data" refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze», James Manyika and others, 'Big Data: The next Frontier for Innovation, Competition, and Productivity | McKinsey' (McKinsey Global Institute 2011) <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation> accessed 7 July 2021. According to the WP29 big data «refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms», Article 29 Data Protection Working Party, 'Opinion 3/2013 on Purpose Limitation' (2 April 2013) WP203.

679 Rouvroy (n 678) 10.

680 Rubinstein defines big data as «data mining on steroids». IS Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74, 76.

681 Mayer-Schönberger and Cukier (n 647) 58; Hildebrandt, 'Defining Profiling' (n 637) 17 ff.; David Bollier, 'The Promise and Perils of Big Data' (Aspen Institute 2010) 16 ff.

682 See e.g., Bernhard Anrig, Will Browne and Mark Gasson, 'The Role of Algorithms in Profiling' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer Netherlands 2008) 65 ff. <http://link.springer.com/10.1007/978-1-4020-6914-7_4> accessed 7 July 2021..

683 European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (19 November 2015) 7.

applications may dramatically improve decisions and discoveries in the areas of scientific and medical research, traffic management or fight against organized crime[684]. Business-related examples of big data applications can already be widely found in the areas of banking and finance; advertising; gross retail and media telecommunication[685].

Big data is not always personal data. A lot of information may be sensor or machine-generated information, or even come from anonymized data sets. However, in both cases re-identification of individuals is nowadays highly feasible. With the advent of smart devices and Internet of Things applications, many information generated and collected from connected devices can be easily related to their users[686]. Anonymization techniques, on the other hand, face intense challenges as a consequence of big data progresses[687]. Growing technical abilities and combination of different data sets, typical of the big data phenomenon, drastically increase the chances of re-identifying single users starting from seemingly anonymous and meaningless information[688]. True anonymization requires renewed efforts and technical abilities that need to be re-assessed and maintained over time[689]. Also, as it will be clarified below, even genuine anonymization cannot protect individuals from some of the consequences arising from big data uses.

3.2.2 Issues: secondary uses and loss of control of profiles

Despite the undisputed individual and social advantages of big data, these new models of processing have raised significant issues in the current data protection framework.

---

[684] For a comprehensive overview of big data applications refer to Omar Tene and Jules Polotensky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 1 Nw. J. Tech. & Intell. Prop. 239, 245–250; Mayer-Schönberger and Cukier (n 647). Also see note (5) of the European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (n 683)..

[685] AGCOM, AGCM, Garante per la protezione dei dati personali (n 649) 18–22; Tene and Polotensky (n 684) 1.

[686] European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (n 683) 7. See *infra* par. 3.3 in this chapter.

[687] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA L. Rev. 1701. According to Ohm, big data enables data controllers to link even more information to an individual's profile, leading to a "database of ruin".

[688] Practical examples of how re-identification of anonymous datasets is easier especially in online environments are provided in Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymisation of Large Datasets. (How to Break Anonymity of Netflix Prize Dataset)' [2008] Proceedings - IEEE Symposium on Security and Privacy 111, 111.;J Bohannon, 'Credit Card Study Blows Holes in Anonymity' (2015) 347 Science 468; YA de Montjoye and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536..

[689] Giuseppe D'Acquisto, Maurizio Naldi and Giuseppe D' Acquisto (eds), 'Anonimizzazione', *Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza* (Giappichelli 2017) 31 ff..

Many scholars believe that even the data protection reform has not adequately considered and tackled the big data phenomenon[690]. The core principles of data protection, such as minimization and storage limitation, are difficult to apply in practice when the big data philosophy has a strong propensity towards data harvesting and favours long retention periods[691]. Transparency and information power are also at risk, given the use of analytics and predictive algorithms that are increasingly impenetrable and feed an opaque decision-making environment (see *infra* para. 3.2 and 3.3). Particularly challenging for the notion of "individual control" and autonomy over data processing, however, are the issues connected with (i) secondary uses of big data and (ii) the advanced profiling practices enabled by big data technologies.

SECONDARY USES - The strength of big data lies in the possibility to extract new (unexpected) knowledge from massive collection of information. This means that, very often, the purposes of processing are not clear-cut at the moment of data collection[692], but only in a second moment, as a result of their further combination, analysis and aggregation[693]. The consequence is the impossibility for data controllers to provide data subjects, at the moment of collection, with a detailed level of information in relation to the objectives of the processing and, consequently, the impossibility for data subjects to take an informed decision[694]. Indeed, the GDPR contains a rule requiring controllers to inform data subjects if they intend to further process the personal data for a purpose other than that for which the personal data were collected in the first place (Art. 13(3)). However, in a big data scenario, this would be either extremely burdensome, given the number of data subjects involved, or unfeasible, since most of the time secondary purposes of data uses are established only after the knowledge extraction, hence only when the new processing has already ended. In addition, since big data are frequently characterized by high rates of data exchanges, they enable the establishment of long and undefined networks of stakeholders involved in data processing, further fueling the transparency issues analysed above.

---

690 *Ex multis* Rubinstein (n 680) 74; Alessandro Mantelero, 'La Privacy All'epoca Dei Big Data' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2019) 1182.
691 Mantelero, 'La Privacy All'epoca Dei Big Data' (n 690) 1190.
692 Mayer-Schönberger and Cukier (n 647) 153.
693 Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1889.
694 Mayer-Schönberger and Cukier (n 647) 153; Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1889.

ADVANCED PROFILING - The abilities to profile individuals and predict their behavior are among the most promising and dangerous uses of Big Data[695].

The practice of profiling is not necessarily connected to the big data phenomenon. Different forms of profiling and categorization have always been carried out, but they generally used a few simple variables, which limited their predictive ability[696]. With big data analytics, instead, the massive volume of information coupled with the increased computing power of new software, has enabled the employment of hundreds different variables thus exponentially expanding the inferring and predictive capabilities.

Broadly speaking, profiling means gathering information about an individual (or group of individuals) to evaluate their characteristics or behaviour patterns and place them into a certain category or group[697]. The GDPR defines "profiling" as «any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements»[698].

Generally, profiling can be distinguished in "individual" and "group"[699]. *Individual* profiling is used to infer specific characteristics (habits, behaviours, preferences, risks) of a single individual[700]. *Group* profiling, instead, is used to find shared features between members of an existing community (e.g., the dress code of students of a class) or to define categories of individuals sharing some common properties (e.g., the high income of people living in a certain neighbourhood)[701]. In the majority of cases, group profiles are "non-distributive", meaning that the member of a group do not share all the

---

[695] Ana Canhoto and James Backhouse, 'General Description of the Process of Behavioural Profiling' in Serge Gutwirth and Mireille Hildebrandt (eds), *Profiling the European Citizen* (Springer Netherlands 2008) 47 ff. The use of algorithmic classification systems and predictive software raises also big issues in relation to the lack of transparency or "explainability" of the logic of the algorithm itself, which exposes individuals to be subject to decisions that they do not understand or of which they are not even aware (see *infra* par. 4.1).

[696] Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 624) 4.

[697] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478) 8.

[698] Art. 4(4) of the GDPR.

[699] Hildebrandt, 'Defining Profiling' (n 637) 20; Valeria Ferraris and others, 'Defining Profiling' [2013] Woking Paper 1 of the EU Project "Profiling - Protecting Citizens' Rights Fighting Illicit Profiling" 6–7 <available at: http://www.ssrn.com/abstract=2366564> accessed 2 December 2021.

[700] David-Olivier Jaquet-Chiffelle, 'Reply: Direct and Indirect Profiling in the Light of Virtual Persons' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer Netherlands 2008) 35.

[701] Hildebrandt, 'Defining Profiling' (n 637) 20.

characteristic of that group profile[702]. For example, the group profile "persons leaving in neighbourhood X have an average earning capacity of Y" does not automatically imply that all families leaving in neighbourhood X have such earning capacity, as other variables may come into play. This kind of profiling has therefore a higher probability of mistakenly identify people as members[703]. However, the more data of different people is analysed, the more the predictability rate of a correlation (neighbourhood – high income) increases. This is the additional value that big data brings to the equation. Another useful distinction in profiling concerns the difference between "direct" and "indirect" profiling, that may apply to both individual and group profiling. If a profile is applied to the same person/group that it was mined from, then it is *direct profiling*, hence it is used to better define the person/group's habits and predict its behaviour[704]. On the contrary, *indirect profiling* refers to the application of a profile to individuals/groups because (some of) their characteristics match the profile, even though the profile was derived from data of different subjects[705].

Essentially, the purpose of profiling is to generate new knowledge about individuals and groups. Profiling allows to infer specific human traits (e.g., personality[706] and emotions[707]) and other sensitive information[708], as well as to predict certain behaviours[709]. The new acquired knowledge can be used to establish benchmarks of "predefined patterns of normal behaviour" against which people can be ranked and

[702] Ferraris and others (n 699) 6. As opposed to "distributive" group profiles, where all members of the group share the attributes of the profile. It is the case for example of the group "bachelors" and the attribute of "not being married".
[703] ibid 7.
[704] Jaquet-Chiffelle (n 700) 40.
[705] ibid.
[706] Yves-Alexandre de Montjoye and others, 'Predicting Personality Using Novel Mobile Phone-Based Metrics' in Ariel M Greenberg, William G Kennedy and Nathan D Bos (eds), *Social Computing, Behavioral-Cultural Modeling and Prediction*, vol 7812 (Springer Berlin Heidelberg 2013).
[707] Wu Youyou, Michal Kosinski and David Stillwell, 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans' (2015) 112 Proceedings of the National Academy of Sciences 1036. The study shows that computer judgments of people's personalities based on their Facebook likes are more accurate than judgments made by their close acquaintances. Similarly, Raina M Merchant and others, 'Evaluating the Predictability of Medical Conditions from Social Media Posts' (2019) 14 PLOS ONE e0215476. The research shows that diseases such as diabetes, anxiety and depression can be effectively predicted from users' Facebook status updated.
[708] M Kosinski, D Stillwell and T Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110 Proceedings of the National Academy of Sciences 5802 <http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110>.The researchers showed that Facebook Likes can be used to automatically and accurately predict a range of highly sensitive personal attributes, such as sexual orientation, political views, use of addictive substances.
[709] Mühlhoff (n 635).

assessed[710], which in turn can be used to inform decisions about individuals and groups, greatly improving controllers' decision-making. These decisions can be legally impactful, for example a hiring based on the eligibility ranking produced by recommending predictive systems[711] or the granting of a loan based on the individual credit scores generated by the profiling customers' economic habits[712] (usually identified as automated decision-making processes[713]). They may also not bear immediate legal effects, but still be very affecting, such as profiling used to personalize customers' service and ads to elicit better engagement or more purchases[714] . Different processing techniques can support the profiling activity, from statistical deduction to advanced computational algorithm, including AI and machine learning[715]. The more sophisticated the technique, the more the knowledge generated from the data analysis may be unexpected and predictions accurate.

From a GDPR perspective, profiling activities, whether or not leading to automated decision-making, are subject to the transparency requirements and the consent of the data subject[716]. When profiling is employed in a *solely* automated-decision making process, further safeguards are provided under Art. 22 GDPR (such matter is dealt separately under par. 3.4 below). However, the new possibilities opened by big data and its derived applications have considerably increased the type and intensity of risks that profiling practices may entail, both for the individual and for the collectivity in general. Risks that individuals have no ability to calculate and hold back, which fundamentally challenge the idea of individual control over their personal data and meaningful consent to data processing in this field.

---

[710] Privacy International, 'Data Is Power: Profiling and Automated Decision-Making in GDPR' (2018) <https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr>.

[711] See e.g. the work of Alex Rosenblat, Tamara Kneese and Danah Boyd, 'Networked Employment Discrimination' (Data & Society 2014) Future of Work Project supported by Open Society Foundations <https://www.datasociety.net/pubs/fow/EmploymentDiscrimination.pdf>.

[712] On "big data" credit scoring, from a US perspective, see Mikella Hurley and Julius Adebayo, 'Credit Scoring in the Era of Big Data' (2017) 18 Yale Journal of Law and Technology <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5>. In the EU, the OpenSHUFA project, jointly conducted by the Open Knowledge Foundation Germany and AlgorithmWatch, seeks to expose the credit scoring practices of the German credit agency SCHUFA, by analysing the collection and processing of German residents' data. Algorithmic Watch, Open Knowledge Foundation Deutschland, 'OpenSCHUFA' (*OpenSchufa*) <https://openschufa.de/english/> accessed 2 November 2021.

[713] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478) 8.

[714] European Data Protection Supervisor, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (n 613) 9.

[715] Privacy International, 'Data Is Power: Profiling and Automated Decision-Making in GDPR' (n 710) 3–4.

[716] Consent is not the only legal ground that justifies profiling activities (e.g., legitimate interest) and automated-decision making processes (e.g., performance of a contract), but it is the one with the broadest scope and frequency of application.

(a) LOSS OF CONTROL ON PROFILES' CONSTRUCTION - Profiling has become so sophisticated in deriving and predicting new unknown (even extremely sensitive) knowledge that individuals are easily unaware of the type of information that the outcome of the profiling activity can reveal about them, regardless of the type of data that they shared in the first place[717]. Studies have shown how easily big data analysis can derive sensitive data (such as illnesses, religious habits, sex) from apparently innocent data sets[718]. Therefore, expectations of individuals at the time they provide their data may not meet the actual results.

A factor that contributes to this loss of awareness comes from the consideration that, in modern information practices, «no personal data remains strictly personal»[719]. The expansive adoption of *group* and *indirect* profiling techniques, that allow controllers to build profiles that can be applied to a broader community of targets, essentially dissociates the data used to create the profile, from the data subjects to whom the profile will be applied. When predictive models and profiles are built from data derived from large pools of people, in fact, one person's data becomes no less significant than another's[720]. In other words: our neighbours' data become as good as our own[721]. Even if one decides to not share his/her own data, there will always be a significant group of people like him/her willing to disclose their data, which will be processed by modern analytics to contribute to the construction of a profile and the training of a model that could eventually be applied and used to the person who opted out[722]. Profiles have no immediate relation with the specific subjects to whom they could be later applied[723].

(b) LOSS OF CONTROL ON PROFILES' APPLICATION - Broader collective issues concern the possibility that profiling practices lead to unfair biased or discriminatory outcomes. Inaccuracies and mispredictions in the profile's construction can lead to biased representation of certain groups and individuals that end up being misclassified and misjudged[724], which in turn may produce potentially discriminatory effects[725].

---

[717] Mireille Hildebrandt, 'Who Is Profiling Who? Invisible Visibility' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 241 ff.
[718] See above notes 707 and 708.
[719] Nadezhda Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (2017) 10 Journal of Law and Economic Regulation 64, 70–71.
[720] Rouvroy (n 678) 22.
[721] ibid.
[722] Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (n 719) 70–71.
[723] Rouvroy (n 678) 22.
[724] Privacy International, 'Data Is Power: Profiling and Automated Decision-Making in GDPR' (n 710) 9.

Equally, “accurate” profiles can conduct to indirect forms of discrimination to the detriment of people that are already marginalized, perpetuating existing discriminatory patterns and social inequalities[726]. And due to the network effects mentioned above, it is sufficient to use the «data from millions of “normal people” who think they have “nothing to hide” »[727] to train algorithms into learning «what “normal” (translate: “privileged”) means so that predictive systems can discriminate against allegedly non-normal, dangerous, sick, [...] persons»[728]. In addition, even in the absence of unfair bias or discrimination, profiles can end up locking individuals in pre-fixed categories, restricting them to their suggested preferences[729] or can be used for manipulative and persuasive purposes[730].

The observations made above lead to a simple (and discouraging) conclusion. Individuals have little awareness, thus control, on the profiles that are constructed about them, due to both the complexity of underlying analytics technologies and the downstream effects that others’ personal data have. As a consequence, they have hardly any perception about the dangers that profiling activities may entail and the harmful consequences that their consent to data processing may cause to them, others and society at large.

3.3 Ubiquitous and opaque data collection

3.3.1 The Internet of (Every)Thing

Technology advances have substantially improved and diversified the ways in which personal data can be collected, making data collection easier, more intrusive and difficult to detect. Further, tech developments and tracking techniques have qualitatively changed human involvement in data collection, making it less and less necessary for people to actively participate (and be aware) of it[731].

A factor that contributed to the emergence of these trends can be traced back in the progressive deployment of sensors in our private and working life, which lead to the

[725] Mantelero, ‘Personal Data for Decisional Purposes in the Age of Analytics’ (n 624) 17–18.
[726] Mühlhoff (n 635) 13.
[727] ibid 14.
[728] ibid.
[729] Article 29 Data Protection Working Party, ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679’ (n 478) 5.
[730] European Data Protection Supervisor, ‘Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data’ (n 613) 9 see also ; Sartor, Lagioia and Galli (n 613).
[731] Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, ‘Privacy in the Internet of Things: Threats and Challenges: Privacy in the Internet of Things: Threats and Challenges’ (2014) 7 Security and Communication Networks 2728, 2733.

development of what is known as the "Internet of Things" (IoT) or, as later labelled, the "Internet of Everything"[732]. There is no agreed definition of IoT. The concept represents a novel technological paradigm based on the idea of increasing miniaturization and availability of ICT at decreasing cost and energy consumption[733]. Hence, its definition is not univocal as it depends on technological progress[734]. Closely linked with the vision of pervasive and ubiquitous computing[735], at the beginning IoT was mainly conceived as a network of sensors enabled by RFID (Radio-frequency-identifiers) and WSN (Wireless-sensor-network) technology[736]. In time, and with the explosion of the Internet, IoT grew to encompass a wide variety of developments, tentatively described as an infrastructure powered by different communication technologies in which «billions of sensors embedded in common, everyday devices – "things" […] – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities»[737]. In other words, today IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world[738]. "Interaction" is therefore a key feature of IoT, understood as interaction with the physical world (to collect data) and with other devices (to communicate, analyse and store data).

Examples of IoT applications cover a wide range of areas and an even broader range of devices[739]. The health and automotive sectors are making great use of networked sensors[740], embedded in wearable devices[741] and quantified-self things[742] used to track

[732] OECD, 'OECD Digital Economy Papers: The Internet of Things: Seizing the Benefits and Addressing the Challenges', vol 252 (OECD 2016) OECD Digital Economy Papers 252 8. Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 87, 89. According to Peppet the term was first coined by Cisco's CEO John Chambers.
[733] Ziegeldorf, Morchon and Wehrle (n 731) 2731.
[734] Federica Giovannella, 'Le Persone e Le Cose: La Tutela Dei Dati Personali Nell'ambito Dell'Internet of Things' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2019) 1213–1214; OECD (n 732) 9.
[735] "Ubiquitous computing" (even known as "pervasive computing" or "ambivalent intelligence") refers to a scenario in which computers are increasingly present in everyday objects, but increasingly less visible to help with everyday functions in an automated fashion. See further Mark Weiser, 'The Computer for the 21st Century' (1991) 265 Scientific American 94.
[736] Ziegeldorf, Morchon and Wehrle (n 731) 2731.
[737] This is the definition provided by Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (16 September 2014) WP 223 4.
[738] OECD (n 732) 1.
[739] For a recent overview of the top 50 IoT sensor applications, see Libelium, 'Report: 50 Sensor Applications for a Smarter World', (9 September 2020)' (Libelium 2020) <https://www.libelium.com/libeliumworld/top_50_iot_sensor_applications_ranking/>.
[740] Peppet (n 732) 98–107.

some aspects or patterns of their users' health or fitness[743]; or as automobile implanted sensors that record car functioning information or track drivers' behaviours[744]. Smart homes, packed with automation and connected devices[745], further embellished with smart grid technologies[746]are also an aspect of this proliferation. Smartphones played also a crucial role in the realization of IoT, being the first mass and ubiquitous devices with embedded sensors[747]. Not every IoT application is concerned with the collection of personal data (e.g., sensors used for whether monitoring or industrial control)[748]. However, as previously mentioned, information collected by environment or machine sensors (like energy consumption data from smart meters; room temperature data from ambient sensors and battery consumption information from smartphones) is increasingly able to identify (and profile) specific users, by looking at the behavioural patterns or individual habits inferred from the data analysis. In particular, the peculiar characteristic of sensor data to capture a rich picture of certain individual characteristics or activities makes re-identification from apparently anonymous data sets easier than expected, severely reducing the chances of true anonymization[749].

IoTs are also one of the most valuable allies of "big data" technologies. The crucial amount of data gathered by these devices feeds the big data ecosystems and supports its continuous growth[750].

---

[741] The WP29 defines "wearable device" as everyday objects and clothes in which sensors were included to extend their functionalities (smart glasses). Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 5.
[742] The WP29 defines "quantified self-things" as devices that are designed to be regularly carried by individuals who want to record information about their own habits and lifestyles (smart watches). ibid.
[743] Peppet (n 732) 98–104. Peppet describes different applications in the health sector including countertop devices, wereable sensors, intimate contact sensors and ingestible/implantable sensors.
[744] ibid 104–117. The author details specific IoT applications in the automotive sector, like event and data recorders, various automobile sensors controlled via smartphone and auto-insurance telematics devices.
[745] The WP29 refers to "home automation" applications or "domotics", Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 6; Peppet (n 732) 108–109.
[746] European Data Protection Supervisor, 'Opinion on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems' (8 June 2012).
[747] Ziegeldorf, Morchon and Wehrle (n 731) 2732; Peppet (n 732) 114–117.
[748] See the detailed list of IoT applications classified under "Smart Environment", "Smart Water" and "Industrial control", Libelium (n 739).
[749] Peppet (n 732) 128–130. The author points out that sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique. Also the WP29 provides an example regarding the «collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals», Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 8.
[750] OECD (n 732) 10.

3.3.2 Issues: big data issues and hidden tracking

"BIG DATA" ISSUES - Due to their strict connection, IoTs share with big data most of the challenges posed to data protection principles (e.g., data minimization and storage limitation principles)[751] and further reduce the possibility for individuals to control and participate in the data processing.

First, IoT developments contribute to enlarge the number of "IoT stakeholders" with device manufacturers, application developers, social platforms and other data recipients[752], contributing to aggravate the control issues reported in previous paragraphs linked to an expansive network of data consumers and growing opportunities for secondary uses[753]. In the same way, proliferation of sensors, that enable the gathering of information from a multitude of devices disseminated in everyone's life[754], greatly enhance the capabilities to refine and enrich "neighbours' data" based profiles and predictive models, adding fuel to the control issue related to profiling and algorithmic described in par. 3.2 above.

HIDDEN TRACKING - Disentangling for a moment the IoT phenomenon from the big data pot, one can identify one further critical pitfall created by the distinctive features of IoT applications. In the field of customer applications, the IoT vision lies in the development of sensors that are undetectable and imperceptible, to have the minimum possible impact on the users' experience[755]. Most devices in which sensors are embedded are not even distinguishable from "normal" non-connected devices, especially in the case of wearables devices, that take the form of watches, glasses or wristbands[756].

The risk of disguise raises important questions on the identifiability of data processing in IoT environments, which in turn has serious consequences on the overall awareness of users and their "bystanders" (i.e., persons interacting with the user of an IoT device) on

[751] Giovannella (n 734) 1222–1223.
[752] Jenna Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) 26 International Journal of Law and Information Technology 45, 47–48.
[753] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 180) 4 and 10-13.
[754] Ziegeldorf, Morchon and Wehrle (n 731) 2735; Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 8. With specific reference to smart meters, see European Data Protection Supervisor, 'Opinion on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems' (n 746) 5.
[755] Giovannella (n 734) 1227; Ziegeldorf, Morchon and Wehrle (n 731) 2733.
[756] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 7.

the occurrence of a data collection[757]. In particular, while users may be generally aware being in presence of an IoT device (because they wear it, have installed it in their house or in their car) but may not have cognition of the exact moment in which the device collects their information, bystanders may be completely in the dark about the very possibility of being in proximity of one of those devices and having their behaviour unknowingly tracked. Lack of control over data collection and flow is even more tangible when smart objects communicate automatically or by default information between each other (so called "machine to machine" or "M2M" communication), typical of IoT devices. In the absence of the possibility to effectively monitor how objects interact o to be able to set virtual boundaries by defining active or non-active zones of collection and communications for certain applications, it becomes extraordinarily difficult to control the generated flow of data[758].

3.4 *Solely* automated decision-making processes

3.4.1 Algorithms, AI and machine learning

As already mentioned above, widespread availability of personal data, number of data sources and advances in big data analytics have paved the way for an extensive use of automated-decision making practices in a number of fields. Automated decision-making refers to operations in which decisions are taken based on automated processes, which can include a previous profiling activity[759] (e.g., a banking system calculates the credit score of a customer and decides whether to accept the mortgage request) or not (e.g., a speeding fine is automatically issued on the basis of the evidence collected from speeding cameras)[760]. Further, the growing complexity of these practices, that makes human contribution less and less relevant, and the speed and efficiency with which they can achieve results has made *solely* automated-decision making processes increasingly popular. This means that the decision is taken exclusively by an algorithm or a machine, with no or trivial human involvement[761]. Banking, insurance and finance are among the

[757] Giovannella (n 734) 1229; Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 7.
[758] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (n 737) 6.
[759] See par. 3.2 in this chapter for the definition of "profiling".
[760] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478) 8.
[761] The WP29 clarified that for a decision-making process to not be fully automated, human involvement needs to be relevant and effective, and cannot be "fabricated". For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. ibid 21. Brkan further stresses that to qualify as human

sectors that make intensive use of algorithmic decision mechanisms[762]. Some scholars argue that most decisions based on a profiling activity should in fact fall under this definition, since the "recommended" results are often not actively reviewed, questioned or influenced by human agents, leading essentially to decisions taken *solely* by a machine[763].

Indeed, Artificial Intelligence ("AI") based systems are already one of the major applications of solely automated decision-making processes. Despite the absence of a generally agreed definition of AI[764], the term can be understood as referring to systems that mimic decision-making abilities of a human being and, given a certain human-defined goal/problem, produce an output, which may result also in a decision, based on the data fed into the system or perceived from the outside environment. Even if the development of systems that can functionally equate human intelligence (so called "general" of "strong" AI) [765] remains at the moment a theoretical possibility and AI

involvement, the controller must ensure that any oversight of the decision is meaningful and is carried out by someone who has the authority and competence to change the decision. Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond' [2017] SSRN Electronic Journal 98.

[762] See in particular Maria Teresa Paracampo, 'FinTech Tra Algoritmi, Trasparenza e Algo-Governanc' (2019) 2 Diritto della banca e del mercato finanziario 213. See also Chiara Alvisi, 'I trattamenti nel settore bancario, finanziario e assicurativo' in Licia Califano and Carlo Colapietro (eds), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (Editoriale scientifica 2017).

[763] In this sense Brkan points out that «it is difficult to imagine examples where person's personal data not leading to profiling would lead to an automated decision. A potential example would be automated application of tax rules in order to determine how much tax return a tax resident would get. However, would that decision again not be based on her personal tax profile?». Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91, 97.

[764] Different scholarly and institutional definitions of AI have been proposed during time, following the advances of the AI sector. The term was first coined by Stanford Professor John McCarthy in 1955 referred to «the science and engineering of making intelligent machines». John McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' 27 AI Magazine 12. Developments and techniques have much advanced since then. At EU Institutional level the most recent definitions include the one provided by the European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe' (2018) COM(2018) 237 final.; by the European Commission's High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Scientific Disciplines' (European Commission's High-Level Expert Group on Artificial Intelligence 2019).; by the European Parliament, 'European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence' (2020) P9_TA(2020)0276. and finally by the European Commission, 'Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2021) COM(2021) 206 final..

[765] "General" or "Strong" AI pursues the ambitious objective of developing computer systems that exhibit most human cognitive skills, at a human or even a superhuman level. "Weak" or "Narrow" intelligence pursues a more modest objective, namely, the construction of systems that, at a satisfactory level, are able to engage in specific tasks requiring intelligence. Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (First edition, Oxford University Press 2014).

applications are mostly used to perform one or more selected tasks, the progresses in this area have made astounding lead forward. Particularly, machine learning (ML)[766] and deep learning (DL)[767] techniques, which provide systems the ability to learn and improve automatically from experience without being explicitly programmed, have revolutionized the ways in which knowledge, patterns and predictions are extracted from existing data sets.

To put it simply, AI applications in their multifaceted forms greatly improve human decision-making, assessment and forecasting processes, even in domains that require complex choices, based on multiple factors, and on non-predefined criteria[768].

3.4.2 Issues: transparency and human intervention

Compared to the "basic" requirements provided for profiling activities and non-solely automated decisions, the GDPR introduced tailored "control measures" to empower individuals when subject to *solely* automated decision-making practices that produce legal effects or significantly affect them[769]. These include enhanced transparency requirements, a specific right not to be subject to solely individual automated decision-making processes but also additional rights, such as the right to require human intervention and to contest the process' results[770].

These safeguards, however, are often compromised by the over-complex and opaque technological processes on which modern algorithmic decision-making is based. In

[766] Through machine learning, systems are provided with learning methods and tasks to achieve, rather than specific rules that instruct them on how such tasks should be achieved, and are then left free to learn how to effectively accomplish these tasks by extracting/inferring relevant information from input data. There are four basic approaches to machine learning: "supervised learning", the machine learns through 'supervision' or 'teaching', consisting in the provision of a training set that contains correct answers; "reinforcement learning" is similar to supervised learning, as both involve training by way of examples, however, in the case of reinforcement learning, the system learns from the outcomes of its own actions, namely, through the rewards or penalties (e.g., points gained or lost) that are linked to the outcomes of such actions; in "unsupervised learning", finally, AI systems self-learn how to achieve the task without receiving external instructions, either in advance or as feedback, about what is right or wrong. Sartor (n 162) 7 ff.

[767] Deep learning is a sophisticated form of machine learning which uses neural networks (i.e. groups of computing nodes inspired by human brain neurons) to further adapt and improve its outputs. Application of deep learning include image recognition and machine translations. Future of Privacy Forum, 'The Privacy Expert Guide To Artificial Intelligence and Machine Learning' (Future of Privacy Forum 2018) 19–20.

[768] Sartor (n 162); Future of Privacy Forum (n 767).

[769] On the difficult interpretation of the term "legal effect" or "significantly affects", see further paragraph 4.1 *infra.*

[770] Art. 22 (3) GDPR states that in case of a solely automated decision «the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least 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».

addition, a number of legal uncertainties also hinder the effective exercise of these rights (see par. 4.1 *infra*).

TRANSPARENCY - Starting from the transparency requirements, Articles 13 and 14 GDPR include an *ad-hoc* specification[771] for controllers to inform individuals (i) on the *existence* of automated decision-making; and (ii) to provide them with at least *meaningful information about the logic* involved, as well as the *significance* and the *envisaged consequences* of such processing for the data subject. The same information requirements are reiterated also under Article 15(1)(f) GDPR, about the right to access, according to which the data subject can actively request controllers the same elements, should they not be provided at the outset.

Despite a vivid academic debate on the meaning of these requirements[772], the provision has been generally interpreted as requiring controllers to provide data subjects, before the decision has taken place, a general explanation covering the functioning and consequences of the algorithmic process[773]. These information requirements aim in fact at addressing the fundamental issue of the "transparency" or "explicability" of decisional processes[774]. Yet, in the context of algorithmic decision-making, genuine and adequate explanations are increasingly difficult to achieve. Two barriers contribute to undermine this objective: a "technological barrier", namely explaining complex algorithmic processes is in certain cases technically unfeasible; and the already explored "human cognitive limitations", that make the provision of "digestible" information very challenging when elaborate processes are concerned.

Transparency and explicability have been interpreted in different fields according to different perspectives. For computer scientists, they relate to the possibility of obtaining understandable models that describe the functioning of AI systems, i.e., the "logic" of a decision process in a technical language[775]. Clearly, this cannot be the type of explanation that satisfies the transparency threshold required by the GDPR. All the elements ("logic", "significance" and "consequences" of the processes) needs to be

[771] Article 13(2)(f) and Article 14(2)(g) GDPR.
[772] The debate is dealt more closely under Chapter III, par. 3.1.
[773] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76, 81; Giusella Finocchiaro, 'Intelligenza Artificiale e Diritto - Intelligenza Artificiale e Protezione Dei Dati Personali' (2019) 7 Giurisprudenza Italiana 1657.
[774] Sartor (n 162) 54.
[775] Riccardo Guidotti and others, 'A Survey of Methods for Explaining Black Box Models' (2019) 51 ACM Computing Surveys 1, 1–4.

easily readable and sufficiently understandable by data subjects[776]. Therefore, rather than from a technical standpoint, aspects of "accessibility" of the provided contents, namely their level of comprehensibility to a general public, are essential to achieve the desired explainability[777]. As already indicated above ("Cognitive Limitations" section), when it comes to providing data subjects with adequate information, there is a natural clash between its accuracy and its understandability. High-level, thus approachable, descriptions on the use of algorithmic processes would not provide individuals with a sufficient level of details to detect unlawful data uses or to appreciate the process' possible harmful consequences[778]. However, the communication of detailed, thus inevitably more technical, explanations would make it very challenging for an average individual to extract any usable knowledge about the algorithmic process.

Additional challenges to the provision of accurate information also arise from the dynamic nature of many algorithms that must be continually upgraded and modified, thus implying an incessant updating of the elements provided to inform data subjects of the system's functioning[779].

At the same time, meaningful explanations are in certain cases practically impossible due to the technical complexities of these decisional algorithms. The employment of advanced machine learning techniques has led to a proliferation of opaque AI-based systems that operate like "black boxes"[780], in that the performances of these systems and their ability to autonomously infer patterns and make predictions increase at an inverse rate to the human capacity of understanding their underlying functioning[781]. The more systems are designed to find their "own way" of achieving certain results and are able to self-learn and improve based on their experience, the harder becomes for humans to trace back the logical steps followed by the machine to produce their outputs[782]. Even developers and trainers of these black box systems are normally uncapable to identify the reasons and criteria according to which these systems took a

[776] Brkan (n 763) 113.
[777] Wachter, Mittelstadt and Floridi (n 773).
[778] Alessandro Mantelero, 'Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies' (Council of Europe 2019) 11.
[779] ibid 12.
[780] "Black box" systems refer to programs that allow to see the input data and output results, but provide no insight on the processes and workings in between those stages. See further Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (First Harvard University Press paperback edition, Harvard University Press 2016).
[781] Sartor (n 162) 14.
[782] Mantelero, 'Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies' (n 778) 12.

specific decision[783]. From this it follows that even purely technical explanations of the machine operability are oftentimes cannot be produced.

HUMAN INTERVENTION - Beside transparency requirements, the GDPR introduces further safeguards when solely automated decision-making processes are concerned. Art. 22 GDPR, in fact, endows individuals with a series of rights that they can exercise when subject to an automated decision-making process, including the right to (i) obtain human intervention; (ii) express their point of view and (iii) contest the decision[784]. The exercise of these rights, however, is deeply affected by the technicalities and complexities that surround algorithmic-based decisions.

The exercise of the actions under (ii) and (iii) is impacted by the transparency level of the automated decision-making process. If data subjects do not receive meaningful information about the decisional process and a sufficient level of details, they do not have visibility nor understand the underlying reasoning of the decisions, which is essential for them to object to the decision and advance solid counterarguments.

The right to human intervention poses also significant practical difficulties. First, there is no general guarantee that systems have been built with the necessary mechanisms to make it technically feasible for a human operator to intervene and review the actions performed by the system in a decision-making process[785]. Secondly, it is questionable that a human operator may have the necessary expertise to understand and possibly change the steps that led to produce the final decision. It is unclear how a person with limited capacities of data analysis may be able to justify the need for the system's result to be changed, particularly considering that the algorithmic may have taken into account a multitude of variables and data to reach a decision[786].

4 Legal and other factors

Beside notice and consent, which are the most representative examples of *ex-ante* control mechanisms, control on personal data is exercised also through other subjective rights that the GDPR grants data subjects. Especially in light of new technological advances, the successful exercise of these rights, such as the right to access or rectification, which provide individuals *ex-post* control measures over on-going data processing, has been recognized as a fundamental component of data subjects'

[783] Brkan (n 763) 117.
[784] Article 22(3) GDPR.
[785] Brkan (n 763) 86.
[786] ibid 87.

empowerment[787]. These rights are designed to reinforce individuals' ability to retain a decisional power on their data: opposing to their on-going processing (e.g., right to object); ensuring that the data processed are accurate and true to their self-representation (e.g., right to rectify or supplement); monitoring and questioning controllers' activities (e.g., right to access; right to request human intervention and oppose final decisions in automated decision-making processes), and, more generally, enabling them to manage and re-use their data as they wish (e.g., right to data portability). Nevertheless, the practical implementation of these rights faces a number of impediments that range from unclear legal interpretations and tensions with concurring rights, to non-compliance of controllers and data subjects' scepticism. These obstacles contribute to downsize the role of data subjects' participation in the governance of their personal data, substantially eroding the principle of individual control.

From a general outset, evidence painfully shows that only few individuals exercise these rights in practice. After the implementation of the GDPR, an increased awareness on subjective rights and raising concerns over poor control over personal data did not automatically move individuals to be more active in the exercise of their rights[788]. As a result, the number of requests individuals submits to controllers, therefore their engagement and participation in the governance of their data, is still very low. Low levels of engagement are influenced by a combination of factors that do not only linked to individuals' laziness or lack of care. The successful exercise of these rights is in fact affected by the attitude of controllers in the management of data subjects' requests, that is often obstructive and dismissive. Empirical studies on the right to access show that the information provided as a result of an access request[789] and the timely response

[787] See e.g. European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (n 683); European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' (n 11); European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (n 11).

[788] Only one in ten respondents have exercised at least one of the GDPR rights. European Commission and others (n 559) 23–24.

[789] Only 22% of responses were deemed adequate in the study conducted by Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4, 4. Whereas only 10% of controllers communicated all relevant aspects of the processing in the study of René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review.

rate of controllers, within the time limits required by law[790], are generally not adequate. Approximately the same discouraging results are seen in relation to the exercise of the newer right to data portability[791].

Against this general background, which applies more or less equally to all subjective rights, the following paragraphs take a closer look at the "legal" barriers connected with the exercise of two important subjective rights, on which EU institutions and authorities have set great expectations.

4.1 Dubious interpretation of the "right not to be subject to solely automated decision-making"

As analysed in Chapter I, Art. 22 GDPR reflects the European scepticism towards decisions taken solely by automated means and the concern to provide data subjects with safeguards that would allow them to screen and influence this type of decisions[792]. For the sake of further analysis, it is worth recalling the text of the norm, which is titled "Automated *individual* decision-making, including profiling" and provides under par. 1 that «the data subject shall have the right not to be subject to a decision based *solely* on automated processing, including profiling, which produces *legal effects* concerning him or her *or similarly significantly affects* him or her» (*emphasis* added).

It has already been discussed under par. 3.4 about the technical obstacles that undermine the effective application of certain measures introduced to mitigate the risks of machine-based decisions ("transparency" and "human intervention"). These are complemented with issues of legal uncertainty over the interpretation of Art. 22 GDPR, only partially sorted out by the guidance of data protection authorities, that have inevitable downfalls on the application of the norm.

From the outset, initial uncertainties focused on the type of "right" that the provision introduced. It was debated, in fact, whether the wording of Art. 22(1) should be

[790] Janis Wong and Tristan Henderson, 'The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR' (2019) 9 International Data Privacy Law 173, 179. The author quotes a survey conducted by Talend in 2018, according to which 70% of the companies surveyed reported they were not able to meet the GDPR-specified one-month time limit (13 September 2018) https://www.talend.com/about-us/press-releases/the-majority-of-businesses-are-failing-to-comply-with-gdpr-according-to-new-talend-research/. The same study was carried out in 2019 confirming the low rates of compliance, with 58% of respondents failing to address requests made from individuals within the GDPR limit (3 December 2019) https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/. Both accessed on 6 July 2021

[791] Wong and Henderson (n 790). The authors found out that 61.3 per cent of organizations answered within a month and 74.8 per cent within a three months period agreed by the GDPR.

[792] Brkan (n 763) 97.

understood as entitling individuals with a right they had to actively exercise (similarly to a "right to object") or, instead, the provision introduced a sort of general prohibition for controllers to take automated decisions (unless lawful grounds, like data subject's consent, existed). These doubts were resolved by the majority of academics[793], further validated by the position of the WP29[794], in favour of the latter position. However, a number of other questions remain still unanswered.

"INDIVIDUAL" - A first issue revolves around the "individual" character of the decisions that fall under the scope of this article[795]. Brkan notices that in line with the general scope of application *ratione personae* of the GDPR, the textual interpretation of Article 22 GDPR seems to exclude "collective" decisions affecting a group of persons linked together by virtue of common traits/characteristics/habits[796]. According to the author, these would be, for instance, decisions on dynamic pricing that calculate the price of a good/service based on the area in which an unidentified number of subjects makes the purchase (i.e., decisions based on indirect group profiling). One argumentation supporting this position was that collective decisions were often not based on personal data, rather derived from the analysis of huge anonymized data-sets, which would exclude them from the scope of the GDPR. Beside the fact that anonymity in a big data world has lost much of its reliability, the gaps in data protection that excluding decisions affecting a group of individuals would produce justifies a flexible construal of the wording "individual decision-making", as encompassing both decisions taken towards a single identified individual or a variety of unidentified ones[797]. However, the fact that clarifications on the extent of the GDPR scope when dealing with collective decisions have not been provided yet, creates legal uncertainties in its practical application. By generalizing this right of individuals to all "collective decisions", the risk would be to render the scope of data protection law too broad, as it may end up covering for example social and policy decisions based on a certain population range that may be argued to be yes collective but also made starting from individuals' personal data. On the other hand, excluding collective decisions (thus narrowly interpreting the "individual"

[793] See e.g., Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law* (Springer International Publishing 2017) 9; Brkan (n 761) 99.
[794] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478) 43.
[795] As reported at the beginning of the paragraph, Art. 22 GDPR is titled "Automated *individual* decision-making".
[796] Brkan (n 761) 100.
[797] ibid 101.

character of the decisions covered by this right) would bear the risk to make data protection too limited, excluding vast portions of controllers' activities from the reach of individuals, to their great detriment.

"SOLELY" - A second point of discussion concerns the term "solely" that limits the scope of the prohibition to decisions that are taken *exclusively* with automated means. This brought up the question on what "level" of human intervention was sufficient to rule out the "exclusivity" character, and whether even a minimal involvement could automatically make a decision not fully automated, thus not covered by Art. 22 GDPR. Initial positions that advocated for a strict reading of the expression "solely", according to which even some nominal human involvement could suffice[798], were contrasted by other views[799] that instead objected to a textual interpretation of the norm. The latter positions found valid support in the Guidelines issued by the WP29[800], where the formalistic approach was rejected and it was affirmed that for a decision not to based *exclusively* on machine, a human operator needed to have (i) the ability and power to evaluate the machine results (even when disguised as mere "recommendations") and (ii) bring an essential contribution to the final decision[801]. This construal aimed at preventing possible circumvention of the norm. However, it has two practical consequences. On the one hand, since algorithmic operations underlying automated recommendation/decision systems are becoming increasingly sophisticated, the involvement of a meaningful human contribution is expected to decrease significantly. As already mentioned before in terms of "human intervention", the issue does not concern only black box and opaque systems, whose functioning is obscure even to technical experts and whose outputs may thus be difficult to assess and if the case reject, but also in relation to explainable but complex systems, for which an "essential" contribution from a human operator in assessing and amending the machine decision may be increasingly difficult to expect. This, in turn, would make the distinction between automated-decisions and other merely "recommending" algorithmic processes particularly difficult to trace, dramatically dilating the scope of Art. 22 to include basically most algorithmic outputs. On the other hand, the "human" threshold that needs to be

[798] Wachter, Mittelstadt and Floridi (n 773) 93; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook* (IOS Press 2012) 50.
[799] Lee A Bygrave, 'AUTOMATED PROFILING' (2001) 17 Computer Law & Security Review 17, 20.
[800] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478).
[801] ibid 20–21.

satisfied for a decision not to be fully automated remains a case-by-case assessment that is left to the controller and, only eventually, to the DPA to establish. This, however, increases the risk of opaque or hidden decision-making practices, where Art. 22 and the connected transparency safeguards may not be applied following the – not fully unbiased – assessment of the data controller, without data subjects having any means to know it.

"SIMILAR SIGNIFICANT EFFECTS" – Beside being *individual* and *solely* automated, to fall under Art. 22, decisions need also to have binding effects on data subjects, which means having "legal effects" or "similarly significantly affecting" him or her. The GDPR does not define the term "legal effect", however there is general consensus that the notion covers decisions that have an impact on a legal position or legal interests of the data subject, as provided by law. Less straightforward is the definition of the type of decision-making or profiling practice that *(similarly) significantly affects* an individual[802]. The WP29 offered some interpretative guidance affirming that the expression refers to decisions that have such intrusive impacts on individuals that could be compared to legal ones[803] and provided a non-exhaustive list of decisions affecting data subjects that could meet this definition (e.g., decisions determining financial circumstances; access to health or education services)[804], which adds up to the examples already included in Recital 71 GDPR (e.g., decisions taken during an automated e-recruitment process). As some noted[805], however, it is not always clear where the boundaries between impactful and non-impactful decisions lie. To take the case of targeted advertising as an example, significant adverse effects have been usually attached when a particularly intrusive advertising practice is in place, that targets vulnerabilities of data subjects (e.g., children) or prevent them from purchasing goods and services due to prohibitively high prices[806]. Yet, with the progresses in targeting technologies, any form of price discrimination, commercial nudging, behavioural advertisements, or neuromarketing could be plausibly said to have a significant adverse effect on the persons concerned, as they all undermine, at some level, individuals' autonomy by limiting their choices or

[802] Brkan (n 761) 100.
[803] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478).
[804] ibid.
[805] Brkan (n 761) 103.
[806] Mendoza and Bygrave (n 793) 89; Wachter, Mittelstadt and Floridi (n 773) 93.

behaviours [807]. This raises the question of what should be the criteria to determine which activities meet the threshold of "significant effect". Some authors argue the existence of a causal link between the mentioned activities and the action of data subjects (i.e., whether the said activity is able to divert individual choices in practice) may provide useful guidance[808]. The downside is that this assessment activity could be conducted only on an ad-hoc and ex-post basis (i.e., when the individual has already been subject and affected by the decision), which would not only be extremely complex, but mostly ineffectual as it would leave the individual exposed to this type of decisions, and only able to ask for restoration from its occurred consequences. Even without relying on a causal link, it is evident that the evaluation of whether a certain decision may have significant effects on data subject remains in practice as cumbersome, as it requires to take into consideration a number of factors that may widely vary from situation to situation[809]. In addition, the fact that the evaluation is subjective and up to the controller to conduct adds a further element of trickiness to the matter. In fact, this increases the risk that processing activities, which are not patently legally binding and rather fall in the grey area of "significantly affecting", are either classified as not relevant to Art. 22 GDPR or wilfully not disclosed to data subjects to avoid triggering the connected safeguard measures.

FURTHER ISSUES - Additional issues to the effective exercise of Art. 22 GDPR may arise from tensions between the right of data subjects and competing rights of controllers. As previously mentioned, the GDPR strengthens transparency obligations and access rights[810] requiring controllers to disclose to the concerned subjects the algorithm functionality ("logic"). These provisions, however, may be substantially limited by the proprietary claims of controllers under trade secrets and copyright law[811]. Data controllers may in fact legitimately oppose to the disclosure of information supposedly

[807] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243, 254.
[808] According to Brkan the criterion could help including under Art. 22 GDPR only activities that have in practice a meaningful impact on subjects. For example, if the data subject ignores a targeted advertising and does not follow up on it, Brkan argues that it is rather difficult to affirm that the advertising significantly affects this data subject. To the contrary, if a person systematically shapes his purchasing decisions on the basis of such targeted advertising, the significant effect would be more easily established. Brkan (n 763) 103.
[809] Mendoza and Bygrave (n 793) 89.
[810] Art. 13(2), 14 and 15 of the GDPR.
[811] See for example Brenda Reddix-Smalls, 'Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market' (2011) 12 UC Davis Business Law Journal 87; Malgieri and Comandé (n 807) 262–264.

revealing algorithm codes, predicted data, analytics and secret business practices, which fall under the protection regime of IP rights[812]. Clearly, controllers could not completely waive the transparency obligations they are subject to under the GDPR and would still be required to provide some information on the general functioning/decision criteria of the processing activity[813]. However, depending on where the needle on the scale between controller's property rights and notice requirement is placed, the granularity of the information provided could be substantially undermined, resulting in very high-level and generic explanations that would be of no real use to improve people's awareness.

Another aspect to consider in the exercise of the sub-set of rights granted by Art. 22 concerns the capability of data subjects to express their point of view and contest the automated decision[814]. It is unclear at the moment what the legal consequences should be when the opinion has been expressed and who should decide if the results are challenged[815]. The absence of institutional guidelines on how the internal procedure should be handled, which is left again to the discretion of controllers, and how the practical (negative or positive) outcomes to data subjects should be formulated increases the possibility of controllers ignoring or only formally taking into account the opinion of the data subject or his claim.

4.2 Challenging exercise of the right to data portability

The introduction of data portability under Art. 20 GDPR was considered a key regulatory innovation[816]. As already briefly pointed out, the primary aim was to enhance data subjects' control over their personal data[817], giving them essentially the possibility to obtain and reuse their personal data for their own purposes across different services[818]. The right to data portability entitles individuals to «receive the personal data concerning

[812] Gianclaudio Malgieri, 'Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data' (2016) 4 Privacy in Germany 133, 133.
[813] Malgieri and Comandé (n 807) 264.
[814] Art. 22(3) of the GDPR.
[815] Brkan (n 761).
[816] Data portability was originally grounded in competition law to address anticompetitive behaviours, as it allows consumer to escape possible "lock-in" effects moving from one service to another. Wong and Henderson (n 790) 177.
[817] Recital 63 of the GDPR; Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480). See also Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 European Law Review 793, 809–810.
[818] Wong and Henderson (n 790) 174.

him or her, which he or she has provided to a controller in a structured, commonly used and machine-readable format» and «to transmit those data to another controller»[819].

The enthusiasm for the disruptive potential of this novel right, as an empowerment tool to promote individual control, was toned down. From the outset, rather than facilitating individual empowerment, the right seemed more concerned to achieve market-based objectives, focusing on higher data mobility and secondary data reuse among data controllers[820], in line with the general objectives of the EU to create a healthy and competitive European data ecosystem. Doubts were therefore expressed on whether data portability fitted the fundamental right nature of data protection or should, instead, be conceived as a data-related form of regulation directed to stimulate competition (preventing lock-in effects) and foster innovation[821]. The already ambiguous nature of this right was combined with complications concerning its legal interpretation and practical enforcement, that played a role in further downsizing its innovative spur.

BLURRED SCOPE – The right to data portability has a smaller scope than other subjective rights (e.g., right to access)[822]. Not only it can be exercised merely when the processing is based on consent or contract, but portability can only apply to data that the data subject «has provided to a controller»[823]. The meaning of the wording "provided" was subject to intense debate[824]. It was not clear whether the term included only "volunteered data", actively and knowingly provided or entered by data subjects; also "observed data", namely data obtained from tracking devices, website or service activities, where users may not be aware that such data is collected; or both the latter together with data "inferred" or "derived" from data originally collected (e.g., assessments, scores, profiles)[825]. The EDPB favoured a broad interpretation of Art. 20, affirming that portable data should cover both volunteered and observed data, excluding from the scope only inferred data, being a by-product of the analysis activity conducted by the controller[826]. Current practice, however, seems reluctant to align with this broad

[819] Art. 20(1) of the GDPR.
[820] Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359, 1398.
[821] ibid.
[822] Sartor (n 162) 57.
[823] Art. 20(1) of the GDPR.
[824] See Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193, 201. The authors distinguish between a more restrictive and extensive approach of the notion.
[825] Sartor (n 162) 57.
[826] Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480).

interpretation. From the controller's perspective, such a wide catalogue of portable information could translate into a duty of transfer (possibly to a competitor provider) of precious competitive assets that were costly to collect in the first place[827]. This is why information, such as web tracking and clickstream data are *de facto* not routinely included in the data sets that consumers can download pursuant to exercising their right to data portability[828]. It remains to be seen whether national and EU judges will embrace such a broad approach[829]. For the moment being, without a specific indication or request in this sense, it is hard to expect controllers will voluntarily choose to disclose it in the future. In addition, no clarification has been provided on the degree and scope to which users are allowed to port their observed data (how granular the information about tracked activities should be?)[830], which further leads to risks of inconsistent application among different actors.

LACK OF STANDARDISATION AND INTEROPERABILITY – According to Art. 20 GDPR, the portable data needs to be provided in a «structured, commonly used and machine-readable format»[831], as a condition for data subjects to be able to transmit them to a different provider. The chosen wording was intended to provide a set of minimal requirements that facilitated the interoperability of data formats used by data controllers[832], while attempting to remain technologically neutral[833]. However, the variety of formats (CSV, JSON, XML etc.) and standards that fall under the mentioned definition and may be used in response to a data portability request poses numerous technical difficulties[834]. Evidence shows that limitations based on technological neutrality and unavailability of standards for measuring the appropriateness of file formats are indeed among the factors that make compliance with this right difficult for controllers[835]. Lack of standardization can thus hinder import and reuse capabilities across services and make it very costly for the new provider to offer a compatible

[827] Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making Data Portability More Effective for the Digital Economy' (Centre on Regulation in Europe, CERRE 2020) 51–53.
[828] ibid 6.
[829] ibid 51.
[830] Graef, Husovec and Purtova (n 820) 1373. The authors argue that it is not clear what degree of controller's input, on top of the raw data, will take data out of the scope of portability. While some cases are clearer (individual credit scores and profiles) others are not (photograph uploaded onto a photo sharing platform using a platform-provided filter).
[831] Art. 20(1) of the GDPR.
[832] Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480) 13.
[833] Recital 15 of the GDPR.
[834] Krämer, Senellart and Streel (n 827) 75.
[835] Wong and Henderson (n 790) 183–185.

interface for data subjects to import their data[836]. Full interoperability, defined as the ability of organizations to exchange information directly between their respective ICT systems[837], would solve the multiple-formats issue and alleviate the operational burden on data subjects to export and subsequently import the portable data. However, in the final version of Art. 20, interoperability has not been included as a mandatory requirement[838], rather only as a "suggestion" and "desired outcome"[839]. Therefore, efforts imposed upon data controllers towards full interoperability of digital systems remain moderate[840].

TENSIONS WITH OTHER RIGHTS – Another aspect that appears as a possible obstacle to an effective exercise of data portability is the potential conflict between data portability requests and other rights, such as data protection rights of different data subjects[841] or property rights of data controllers (e.g., IP rights)[842]. Starting from the former, there may be cases in which data of individuals different from the applicant may be caught in the stream of information because they are inseparable from the latter, such as when the request concerns an address book, or pictures in which other people are tagged[843]. This clash of multiple (possibly opposed) interests makes the exercise of this right problematic. Despite the additional economic burden, the provision may indeed encourage data controllers to implement technical measures that allow to segregate (as long as possible) in separate "containers" the personal data of each data subject[844]. However, the risk of future privacy claims may on the other hand discourage providers from accepting import requests.

Tensions with IP rights may also limit the exercise of portability rights. Despite many data assets by firms are IP-free, as they do not meet the required protection

[836] Krämer, Senellart and Streel (n 827) 76.
[837] Annex 2 of the European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards Interoperability for European Public Services' (2010) COM/2010/0744 final. The Annex refers to the definition of interoperability provided by the European Interoperability Framework.
[838] Recital 68 and Art. 20(2) of the GDPR clarify that direct transmission of data from a controller to another can be requested only «where technically feasible».
[839] Recital 68 GDPR; Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480).
[840] De Hert and others (n 824) 200.
[841] Krämer, Senellart and Streel (n 827) 76; De Hert and others (n 824) 198.
[842] Graef, Husovec and Purtova (n 820) 1374; Article 29 Data Protection Working Party, 'Guidelines on the Right to "Data Portability"' (n 480).
[843] Krämer, Senellart and Streel (n 827) 75.
[844] De Hert and others (n 824) 198.

threshold[845], for those that qualify under IP protection (copyright, *sui generis* database right, trade secrets) controllers could invoke their property rights to protect their investments and competitive advantage[846]. It is still unclear the exact interplay between IP and portability rights. The extent to which data subjects are able to transfer their personal data to another provider depends thus on how the balancing with IP law will be conducted in practice[847].

OTHER LEGAL ISSUES – Finally, given the novelty of the right to data portability, organizations have raised some legal concerns with respect to liability issues for data loss and modification during the transfer process[848]. According to the WP29, responsibility is vested in the transferring service provider in the course of the transmission phase, whereases it lies on the recipient provider when data arrives to their destination[849]. However, some noticed there may be instances in which the boundaries between these liability regimes become blurred, making it difficult to determine which activities fall under whose responsibility or giving rise to a co-responsibility[850]. Lack of legal certainty in such a sensitive area may have a dramatic chilling effect over data portability requests.

5 Conclusions

Even if the roots of the idea of individual empowerment and control over personal data lie deep in data protection history, this Second Chapter has shown how this concept is increasingly questioned in light of the challenges that stem from both individuals' inherent limitations, growing complexities of a data-driven environment and legal uncertainties undermining its effective implementation.

At this point, it may be helpful to briefly condense the main findings of the analysis carried out so far in Chapters I and II, to set a few key pillars before moving forward to the next chapters. This conclusive paragraph seeks to briefly summarize the main reasons that have made the concept of “individual control” such a grounding and appealing concept in the data protection framework and further schematically trace its most evident weaknesses, which may ultimately nullify its core objectives.

[845] Graef, Husovec and Purtova (n 820) 1337.
[846] ibid 1379–1386.
[847] ibid 1378.
[848] Krämer, Senellart and Streel (n 827) 76.
[849] Article 29 Data Protection Working Party, ‘Guidelines on the Right to “Data Portability”’ (n 480). 6-7.
[850] The White Paper published by Facebook on data portability provides an overview of these doubts with reference to different transfer models e.g. open transfer, conditioned transfer or partnership transfer. Erin Egan, ‘Data Portability and Privacy’ (Facebook 2019).

5.1 The reasons behind the individual control model

Drawing inspiration from the analysis of the data protection framework developed in Chapter I, a primary aspect that emerges as a decisive contributor in the consolidation of "individual control" as a pillar of data protection is linked to the underlying values, rights and freedoms that have been identified as primary concerns of data protection laws and have been attached to the emergence of the fundamental right to data protection.

(i) INDIVIDUAL SELF-REALIZATION – The fundamental rights-based turn that data protection laws took starting from the '80s; the linkage between data protection and the implementation of values concerned with individual self-development and determination and, as a consequence, the increased pressure to see individuals not as mere passive subjects of protection but pro-active agents in matters concerning their personal data have provided the bases for the arguments in favour of a conceptualization of data protection in terms of "individual control over data flows".

As already discussed in Chapter I, the season that gave prominence to the active role of data subjects within the data protection framework started with the shift towards a more "individual rights" rather than "functional" approach to data processing issues, that marked the introduction of a growing number of subjective rights, designed as participatory instruments for data subjects to exercise a degree of outflow and inflow control over information relating to them[851].

This re-orientation of the data protection discussion paved the way for the emergence of a prominent group of values linked to the development and realization of the person that, despite a lack of uniformity across jurisdictions, became strongly associated with the protection of personal data and grew to be fundamental underpinnings of the right to data protection. The latter was interpreted as a response to the technological progresses with the objective of safeguarding and fostering individual autonomy, self-determination and free development of one's personality[852]. These are human values whose realization is intrinsically connected to the ability of individuals to make independent choices and personal decisions about themselves. In a society where the individual "Self" breaks down in multiple information bits, these values have been

[851] See above, Chapter I, par. 3.2. According to Van der Sloot this regulatory change is the expression of a broader European policy trend to elevate individual rights and consumers' empowerment. van der Sloot (n 621) 321.
[852] See Chapter I par. 2, 3.2., 3.3. and 6.

naturally translated into the idea of "informational self-determination"[853], understood as the ability of individuals to exert a level of control over data that represent them and the consequences that the use of those data may imply[854]. Essentially, the connection between the right to data protection and the pursuit of fundamental values that entail a level of human agency and autonomy has made the control individuals can exercise over their personal data a necessary pre-condition to achieve those values. Therefore, the prominence acquired by the concept of "individual control" in the data protection domain, and the relevance of the individual mechanisms (i.e., consent and other subjective rights) that enable its exercise, is closely linked to the idea that only when individuals have the power and autonomy to decide what personal data they want to share; monitor why and how it is processed and most of all react when it is not processed in the way they expect it to be, they can freely be and develop as human beings.

To this first consideration, at least two other observations can be added to explain the appeal exercised by the notion of individual control.

(ii) WIDESRPEAD CONTROL NETWORK – Reliance on the power (and responsibility) of individuals to exercise their subjective rights, to keep track of processing activities and challenge them when they are not compliant with the expectations establishes, *de facto,* a widespread control mechanism that serves as first monitoring filter to ensure that processing activities are fair and compliant. Data subjects basically create a dynamic network of "alarm sensors" to help oversee controllers' activities and detect unconformities of the data protection ecosystem. Already back in 1995 Rodotà underlined, «it is precisely the presence of this *[widespread extensive control]* that makes it possible to already have in the system an antidote for cases in which the formal control *[by the DPA]* becomes sclerotic or is influenced by public or private pressure groups»[855]. From this perspective, data subjects, being the closest and more direct link to the reality of data processing, should be in a privileged position to overlook the fairness and lawfulness of processing activities, becoming front-line privacy watchdogs in the functioning of the data protection system.

[853] As mentioned in Chapter I, par. 3.3, the concept was coined by the Constitutional German Court in the famous 1983 "census decision".
[854] Rouvroy and Poullet (n 48) 52–54.
[855] Rodotà, *Tecnologie e Diritti* (n 56) 94.

(iii) APPEALING EXPEDIENT – On a less commendable note, the second observation points to the strategic role that the prominence conferred to individual control may play both at political and business level. As it was previously mentioned, the enthusiasm for data subjects' empowerment and the support for enhanced control instruments has been progressively expressed by EU policymakers, but it has more recently been embraced also by the tech industry.

At EU level, calls for strengthening the ability of individuals to control their personal data have been predictably raised by the EU Commission at the dawn of the big data protection reform[856] and were then translated into the GDPR regulatory efforts in reinforcing the subjective rights catalogue. But even tech giants have started to publicly engage with the "control over personal data" mantra. Twitter, Facebook, Amazon and Apple[857], all seem to deeply support the users' cause and have become impatient to provide them with tools to «put them in control» or give them «meaningful choice and control» over how a company may use their data.

Truth is that the rhetoric of individual control can also be used as an appealing expedient that does not work in favour of data subjects. On the one hand, focusing on the enhancement of the powers and means provided to individuals may be a convenient

[856] See e.g., European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (n 11), that states «individuals have the right to enjoy effective control over their personal information». See more recently also, European Commission, 'Communication from the Commission to the European Parliament and the Council. Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' (2020) COM/2020/264 final.

[857] W Hartzog, 'The Case Against Idealising Control' (2018) 4 European Data Protection Law Review 423, 423–424. The author quotes specific interventions made by representatives of big tech companies. In particular, Jack Dorsey, Twitter CEO, saying during an interview at Wired 25th Anniversary Festival «I do believe that individuals should own their data and *should have the right to have the controls over how a company might utilize that* and how a service might utilize that and be able to pull it immediately»; Mark Zuckerberg, Facebook CEO, that in a written testimony for the House Energy and Commerce Committee hearing on 11 April 2018, in the aftermath of the Cambridge Analytica scandal, repeatedly claimed «this is why we work hard to communicate with people about privacy and build controls that make it *easier for people to control their information* on Facebook», https://energycommerce.house.gov/committee-activity/hearings/hearing-on-facebook-transparency-and-use-of-consumer-data-full-committee ; Andrew DeVore, Amazon Vice President and Associate General Counsel, who in written testimony to US Senate Committee on Commerce, Science, and Transportation for September 26, 2018 hearing said «from early-stage development, we built privacy deeply into the Echo hardware and Alexa service by design, and we *put customers in control*», https://www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy ; and Bud Tribble, Apple Vice President of Software Technology, who in a written testimony to the US Senate Committee on Commerce, Science, and Transportation for September 26, 2018 hearing wrote «when we do collect personal information, we are specific and transparent about how it will be used. We do not combine it into a single large customer profile across all of our services. We *strive to give the user meaningful choice and control over what information is collected and used*», https://www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy .

excuse for policymakers to avoid more complex and thorny discussions on the bigger issues raised by modern data processing activities. Offering people "individual control" as an effective instrument to contrast unlawful and harmful uses of personal data may result in dumping a considerable share of responsibility on data subjects, freeing policymakers from the uncomfortable position of having to juggle between the implementation of costly mechanisms or stricter rules to tackle the risks currently posed by modern data processing[858] and the happiness of the industry. At the opposite side of the spectrum, reliance on "individual control" may have its advantages for tech companies as well. When the type of control users have is granted in a context that does not allow it to be enacted effectively, as it happens today, companies have all the interest in maintaining the focus on the idea of data subjects' empowerment. If data protection requires from controllers only "more control" for data subjects, they are happy to fulfil these wishes when this means providing users with more settings, buttons and tools that instil an increased perception of control, without actually making the difference. As Hartzog states, «when control is the North Star, company leaders […] aren't given much to work with when tasked with improvement»[859].

5.2 The limitations of the individual control approach

The analysis conducted in this chapter makes it painfully clear that, as of today, there are not the conditions to regard *real* individual control over information flows as a realistic option, when considered in isolation. The digital environment and modern data practices radically undermine the premise of autonomy and active agency that this notion implies[860]. Several reasons have emerged in support of the affirmation that individual control alone and as exercised today *cannot* be a valid approach for individuals to express their privacy preferences, nor to safeguard them from the risks and harms of data uses. These can be essentially grouped under three main headings.

(i) CONTROL AS AWARENESS – The concept of control assumes that individuals understand and are able to assess the consequences that may result from processing activities, in order for them to make conscious choices about whether to disclose their personal data, accept certain data uses, or even challenge processing practices when

[858] Rodotà, *Tecnologie e Diritti* (n 56) 35. Rodotà, already back in the 1995, warned that «the exclusive insistence on the means of individual control may well be the alibi of a public authority wishing to evade the new problems caused by the large-scale collection of information, and which thus takes refuge in an illusory exaltation of the powers of the individual, who will thus be entrusted with the management of a game that can only be a loser».
[859] Hartzog (n 857) 431.
[860] Lazaro and Le Métayer (n 31) 29.

they harm them or are not carried out according to the initial expectations. The issue is that the level of awareness and the evaluation capacity that would be required to assess and understand the threats posed by data practices cannot be realistically achieved by the average (but also more expert) individual, especially in light of the structural factors characterizing the contemporary digital environment. We are simply not designed, nor equipped to cope with the astonishing complexity and scale of modern personal data processing.

Knowledge limitations, time constraints and cognitive biases inherently affect the rational capacity of individuals to take informed decisions, especially when the perceived threats of most data processing activities remain a distant and indirect factor[861]. The size, complexity and speed of data processing exacerbate these human limitations, further widening the understanding gap of end-users with respect to the real purposes and effects of data uses[862]. In addition, controllers have learnt how to exploit these vulnerabilities to their advantage, through the employment of dark patterns and other misdirection nudges that can alter individuals' privacy concerns, and unconsciously manipulate their choices[863].

(ii) CONTROL AS EFFECTIVE INFLUENCE – The notion of control implies also that individuals, who exercise it, are in a position to exercise it effectively, namely to give concrete voice to their preferences and to have a real influence on the processing of their data. Yet, even in a small-scale and neutral scenario in which individuals are provided with the capacity to be reasonably aware of data processing consequences, therefore more conscious and rational about their choices, many practical and legal obstacles stand in the way of granting data subjects effective instruments to exercise this type of control.

The absence of real alternatives but a "yes or no" option when it comes to decide whether to accept a certain data use ends up belittling individual privacy preferences, eventually forcing individuals to make choices that do not reflect their real intentions[864]. Lack of cooperation by data controllers, that hamper or delay the effective exercise of data subjects' rights, as well as other substantial burdens that data subjects need to face to successfully uphold their requests, create practical barriers to the exercise of

[861] See, Chapter II, par. 2.1.
[862] Chapter II, par. 2.2.
[863] See above Chapter II, par. 2.1.
[864] See Chapter II, par. 3.1.

any form of effective control on any data processing operation[865]. Additional legal uncertainties that surround the application, especially of those subjective rights of more recent introduction, further undermines the ability of individuals to make use of the control instruments they are in theory provided with[866]. In other cases, lack of control derives from a lack of legal instruments to claim it, such as in the case of profiles and predictive models created or enriched with personal data of other people and more generally the inferred and derived knowledge extracted from the profiling activity[867].

In brief, privacy threats are either «hidden through abstraction or made so explicit and voluminous we don't even know where to begin»[868].

(iii) EXTERNALITIES ON THE COLLECTIVITY – A further argument to downsize the role of individual control concerns the fundamental mismatch between its individualized focus and the broader collective and social effects of data processing.

Data protection is a value that transcends the individual dimension, as it serves higher collective and societal goals, (e.g., prevention of discrimination; promotion of creativity; freedom of association) all of which are essentially aimed at preserving the democratic functioning of our society[869]. Therefore, while privacy choices, individually considered, may be perceived as having an effect limited to the concerned data subject, when taken collectively they may greatly impact on common and collective values that concern society at large. From another angle, the collective dimension emerges even more prominently in the context of advanced profiling techniques, that make it possible to predict and infer information of an individual, based on personal data collected and shared by others[870]. In this case, the harmful effects that the choices of an individual (to share his data, to be profiled) have on a multiplicity of other unaware individuals or groups have visible and direct.

However, when individuals make personal choices about their data and exercise their subjective rights, they do not take into consideration the externalities that these actions generate. Individual decisions inherently focus on the individual interests of each person, which may in turn be different or even in contrast with the interest of other

[865] Chapter II, introduction of par. 4.
[866] See in particular the considerations in Chapter II, par. 4.1 and 4.2.
[867] Chapter II, par. 3.2 on the profiling possibilities enabled by big data and modern analytics techniques.
[868] Hartzog (n 857) 429.
[869] As explored in Chapter II, par. 2.3.
[870] See above Chapter II, par. 3.2.

individuals or society as a whole. In this sense, «trusting the wisdom of millions individual choices»[871] to ensure that broader collective and social values are protected is not a suitable option.

Below a schematic summary of the mentioned shortcomings.

Factor	Consequence	Individual Rights Impacted
Cognitive	- Lack of time resources - Poor understandability of privacy notices - Poor privacy literacy - Bounded rationality & judgment biases - Nudges - Externalities of privacy choices	- Transparency (consequently, exercise of other subjective rights) - Consent
Systemic	- Extensive chains of stakeholders - High data mobility and re-use - Difficult allocation of privacy qualifications - Lack of genuine choices - Advanced profiling and predictive models - Ubiquitous and invisible data collection - Impenetrable algorithmic decision-making processes	- Transparency - Consent - General loss of control over profiling activity - Right to request for human intervention - Exercise of subjective rights
Legal & others	- Lack of legal certainty - Tensions with other rights	- Subjective rights (right to access, right to data portability, right not to be subject to automated decision-making processes)

Table 10. Cognitive, systemic, legal shortcomings of individual control

5.3 Should we get rid of "individual control" for good?

The evident pathologies affecting an approach based on individual control have raised doubts on whether this concept should be considered exhausted and unrealistic in the

[871] Hartzog (n 857) 430.

modern data processing context[872]. Questions on whether privacy self-management needed to be abandoned in favour of a more paternalistic regime, leaving only the law to mandate or restrict data processing activities, have surfaced academic literature[873],

Depriving individuals of the right to choose, monitor and challenge how their personal data are shared and used cannot be the final solution, simply because it appears to eliminate at the roots many of the issues reported above. The ability of people to decide freely, even when it comes to the disclosure, use and governance of their personal data, is a fundamental expression of their rights to autonomy and self-determination. Individual autonomy and informational self-determination are values deeply rooted at the core of data protection objectives[874]. Abandoning these values altogether, in the name of a higher protection of individuals, would radically subvert the European traditional approach to data protection, and fundamentally undermine some of its core foundational values. In a world where decisions that affect individuals are taken based on information bits that concern, identify and describe them as persons, safeguarding their right to "have a say" on how their data is used is key to protect a minimal space of autonomy[875].

Further, the primary regulatory alternative to replace individual control would be for law to regulate, authorizing and banning data uses, overriding individuals' freedom to choose. Scholars have strongly counselled against overly paternalistic regulations that, beside curtailing individuals' autonomy, have their own set of issues. Above all, the law should comprehensively determine which data uses are good and which are bad. As Solove asserts, however, «the correct choices regarding privacy and data use are not always clear»[876]. Many of these decisions are subject to very personal cost-benefit analysis, that may vary from subject to subject depending on his personal inclinations, wishes and circumstances. Some people may have an interest to share certain information that others may feel too personal to disclose; some people may want to benefit from targeted marketing, while others not. More generally, data processing are contextual in nature and the beneficial of harmful consequences of data uses often

[872] Hartzog (n 857).
[873] See e.g., Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1894.
[874] González Fuster (n 59); Lynskey, *The Foundations of EU Data Protection Law* (n 44); Rodotà, 'Data Protection as a Fundamental Right' (n 56).
[875] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1899.
[876] ibid 1896.

depend on a complex sum of factors and circumstances that becomes particularly challenging to establish upfront[877].

The argumentations above should neither be used to ignore the manifold problems that individual control experiences, nor to demonize any form of more interventionist regulation on the matter. Concluding that elements of control have a rightful place in data protection law and should not be entirely eradicated, the path forward requires awareness and acceptance of the limits of the individual control model in place and efforts to mitigate such limitations, leveraging supporting and complementing tools.

On the one hand, individuals' effective agency over personal data should be pursued by acknowledging the complex features of the socio-technical context in which individuals act and take decisions, thus seeking for additional mechanisms that meet their needs and adequately support their control faculties.

On the other hand, the rhetoric of empowered individuals should not be over-stated and overly relied on. Inherent limits of the individual control model can be mitigated only by thinking outside the strictly “individual-centric” box, through mechanisms that supplement this approach, making up for its shortcomings.

[877] Moerel and Prins (n 634); Calo (n 570) 1057.

CHAPTER III – Supporting the individual control model

1 Introduction

The numerous challenges that individuals face in the modern technological context, which translate into a general lack of control over the processing of personal data, require to take serious steps to determine what can be improved to restore individual empowerment and where other measures should instead be preferred to compensate for its insurmountable shortcomings.

The Third Chapter and Fourth Chapter seek to explore different mechanisms and approaches that, if adequately leveraged and implemented, could offer effective support and complementation to the individual control model, with a view to increase the level of protection offered to individuals.

Before starting with the investigation, a few preliminary considerations on the work needs to be made.

First, the analysis conducted in the following chapters is not intended to provide an exhaustive taxonomy of the possible measures available, currently or in the future, to support and supplement the individual control approach. Due to time and space constraints, the survey will focus on a selection of measures, either already in place or simply proposed, to provide an overview of the possible alternatives that could be considered and properly upheld to address data subjects' limitations.

Secondly, each measure should not be considered as a one-fit-fit for all solution to the manifold cognitive, technological and legal issues of the individual control model. As the analysis will show, each measure often is designed to target one or a selected number of specific aspects/issues. However, the combined contributions of all or some of these mechanisms may help to develop a more comprehensive response to tackle the analysed shortcomings on different fronts.

Upon these premises, this Third Chapter deals with measures that aim at strengthening the control individuals can exercise on their personal data, by expanding the toolkit they are provided with to maintain agency over processing activities. The common trait of such mechanisms is thus their "individual-centric" focus. The objective of these measures is in fact to enhance the means that individuals can use to gain effective overview and influence over the circulation of their personal data. Therefore, this

chapter takes into consideration measures in relation to which data subjects remain the leading actors and who are still expected to take action individually to protect their own interests.

2 Technological solutions and human-centred design

2.1 Privacy Enhancing Technologies (PETs)

By the late 1990s, the awareness that regulation and policy alone could no longer be sufficient to safeguard privacy was growing[878]. With the increasing complexity and interconnectedness of information technologies, the belief that «nothing short of building privacy directly into system design would suffice»[879] was already consolidating. The initial "defensive" approach towards technology and the risks to data protection that could arise from its use started to be abandoned[880]. As a specific ramification of the broader debate on the "*lex informatica"*[881], the privacy field began to explore technologies that were built into systems to enhance privacy rules and ensure better compliance with regulatory principles ("Privacy enhancing technologies", or "PETs")[882]. Despite the development of different PETs, according to Cavoukian[883] an overall framework that guided the embedding of privacy requirements into systems was still lacking: this is why she developed the concept of *Privacy by Design* (PbD)[884]. PbD

[878] Ann Cavoukian, *Privacy by Design. From Rethoric to Reality* (Information and Privacy Commissioner of Ontario, Canada 2014); Joel R Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 911.

[879] Cavoukian (n 257) II.

[880] Bravo (n 424) 790. This approach was replaced with a more "optimistic" attitude that saw in technology not only a major threat for individuals, but also a useful complement to the effective protection of their personal data. Roberto D'Orazio, 'Protezione dei dati by default e by design' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), *La nuova disciplina europea della privacy* (Wolters Kluwer 2016) 100–101.

[881] According to the proponents of the *lex informatica,* the information society poses new regulatory challenges which can be overcome only by a new "rulemaking" source: software code. While regulation in real space is primarily regulation that relies upon the cooperation of individuals, the code in cyber space (software) can enforce its control directly. Code as in software rather than code as in law would perfectly assure its own obedience and efficiently achieve regulatory objectives. From here, the notorious quote of Lessig "Code is Law". See Lawrence Lessig, 'Reading The Constitution in Cyberspace' [1997] SSRN Electronic Journal <http://www.ssrn.com/abstract=41681> accessed 10 June 2021; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999); Aron Mefford, 'Lex Informatica: Foundations of Law on the Internet' (1997) 5 Indiana Journal of Global Legal Studies 211, 211 ss; Reidenberg (n 878) 911 ss.

[882] Among the first works on PETs, see Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 553; Herbert Burkert, 'Privacy-Enhancing Technologies: Typology, Critique, Vision' in Philip E Agre and Marc Rotenberg (eds), *Technology and privacy: the new landscape* (MIT Press, Cambridge, MA, USA 1997).

[883] Dr. Anne Cavoukian is the former Ontario's Information and Privacy Commissioner.

[884] Ann Cavoukian, 'Privacy by Design. The 7 Foundational Principles.' Information and Privacy Commissioner of Ontario, originally published in 2009, revised in 2011; Peter Hustinx, 'Privacy by Design: Delivering the Promises' (2010) 3 Identity in the Information Society 253.; D'Orazio (n 880) 79; Bravo (n 424) 775. See for a more critical view Ugo Pagallo, 'On the Principle of Privacy by Design and Its Limits:

identifies a general approach, based on seven foundational principles[885], that epitomizes the idea of protecting privacy by embedding it, from the outset, into the design specifications of information technologies, business practices and networked infrastructures[886]. The concept represents a significant shift from traditional models of protecting privacy that previously had focused on providing minimum standards of protection, while PbD, on the contrary, requires a proactive behaviour of controllers[887]. Over the past years, following the increase of online threats to data protection, PbD has steadily gained momentum, being the object of intense institutional debate[888] and eventually recognized as a "basic principle" of data protection[889]. With the EU data protection reform, PbD has been formally codified under Art. 25 GDPR, next to the other basic principle of "Privacy by Default"[890], and requires data controller to «implement appropriate technical and organisational measures […] which are designed to implement data protection principles», both in the design and in the processing phase[891].

Within the overarching framework of the PbD principle, which remains technology neutral, the landscape of PETs, as practical implementation of the PbD approach, has developed fast. PET is an umbrella concept covering a broad range of technologies that are designed to support privacy and data protection[892]. In the absence of a formalized

---

Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer Netherlands 2012).

[885] The 7 foundational principles of PbD are: 1) Proactive not Reactive; Preventative not Remedial; 2) Privacy as the Default Setting; 3) Privacy Embedded into Design; 4) Full Functionality – Positive-Sum, not Zero-Sum; 5) End-to-End Security – Full Lifecycle Protection; 6) Visibility and Transparency – Keep it Open; 7) Respect for User Privacy – Keep it User-Centric. Cavoukian, 'Privacy by Design. The 7 Foundational Principles.' (n 884).

[886] Cavoukian, *Privacy by Design in Law, Policy and Practice* (n 424) 3.

[887] ibid.

[888] In Europe different EU Institutions endorsed PbD, e.g. Article 29 Data Protection Working Party and Working Party on Police and Justice (n 11) 3, 6, 8, 12–15; European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy' (18 March 2010).

[889] Hustinx, 'Privacy by Design' (n 884) 254.

[890] According to the principles developed by Cavoukian, "Privacy by Default" is one of the seven principles underlying privacy by design, that requires systems to ensure an automatic or "default" protection of personal data, regardless of any action of the individual. Therefore, the principle is a pre-requisite for an effective implementation of PbD itself. EU legislators, however, have decided to devote a specific paragraph to this principle, in Art. 25(2) GDPR, right under the paragraph establishing the basic requirements of PbD.

[891] Recently the European Data Protection Board issued guidelines on data protection by design and by default to provide further guidance on the interpretation of the requirements set by GDPR. European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020).

[892] PETs have been defined in numerous ways. For example, the EU Commission, recalling a definition first employed by the EC funded Pisa project, states that «PET stands for a coherent system of ICT

classification of PETs, searching for common denominators, Rubinstein has classified them into two categories: *substitute* PETs (which seek to protect privacy by blocking or minimizing the collection of personal data, thereby making legal protections superfluous)[893]and *complementary* PETs (which are instead designed to implement privacy statutory principles and legal requirements)[894]. Within this last category, PETs can be further distinguished into *privacy-preserving* PETs[895], which resemble substitute PETs in that they mostly rely on cryptography protocols that provide strong privacy safeguards but also satisfy legal requirements, and *privacy-friendly* PETs.

2.1.1 Privacy-friendly PETs to improve control management

Privacy-friendly PETs are a particularly interesting group of technologies for the purposes of our work, as they identify applications that seek to give people more control on their personal data. Their ultimate goal is to overcome some of the cognitive and technological obstacles, described in the previous chapter, that make the practical exercise of subjective rights incredibly problematic, and establish a new "user-centric" ecosystem of data governance. Although talks on the benefits of PbD and PETs have been going on for quite some time, the development of operative tools that can translate these concepts into practice is still in its infancy. A call to increase the efforts in the deployment of PETs has been heavily supported by EU Institutions[896] in light of their potential to address some of the concerns over the loss of individual control over personal data.

---

measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules». European Commission, 'Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)' (2007) COM/2007/0228 final. For an overview of some of the definitions of PETs see further, Marit Hansen, Meiko Jensen and Jaap-Henk Hoepman, *Readiness Analysis for the Adoption and Avolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan : Approved, Version 1.0, Public.* (European Network and Information Security Agency 2015) 10.

[893] Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 Berkeley Technology Law Journal 1409, 1417.

[894] ibid 1418. For an overview of practical examples of PETs in the big data context, see Giuseppe D' Acquisto and others, *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics.* (European Network and Information Security Agency 2015) par. 4.

[895] Rubinstein (n 893) 1418.

[896] See European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Thriving Data-Driven Economy' (n 642) 10; European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (n 683) 13–14; European Data Protection Supervisor, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (20 October 2016).

Privacy-friendly PETs, that may also be referred to as "privacy management tools" (PMTs) or "privacy information management systems" (PIMs)[897], encompass different applications.

A first set of these technologies includes mechanisms that enable individuals to set and record their privacy preferences in advance, before any data processing begins, and then automatically apply them when necessary. Examples of this type of solutions can range from browser-based cookie managers, additional browser controls (e.g., "private browsing" and "do not track" tools)[898] to sticky policies that allow to attach privacy preferences to specific data sets[899]. A practical effort to materialize this approach was made by the Platform for Privacy Preferences (P3P) Project[900], a protocol that required websites to declare their intended use of information they collected about the web browsing history of users and allowed users to determine in advance their own set of "policies", establishing which of their browsing information could be seen and made available to third parties. In this way, users did not have to read privacy policies in every site they visited, since their preferences would be automatically implemented, and websites could automatically obtain the user's information if they met the user's preferences. Despite the initial enthusiasms, the project did not reach the hoped success: very few browsers followed with its implementation[901], that was in any case later removed.

Another more structured set of PETs, often referred to with the terms "data vaults", "data spaces" or "personal data stores" (PDSs)[902] (hereinafter, "PDSs"), relates to

[897] The German Federal Government's Data Ethics Commission states that when the focus is on the provision of technical applications the term PMTs is used, when instead the focus is on the service end, it is more common the use of the term PIMS. German Federal Government's Data Ethics Commission, 'Opinion of the Data Ethics Commission' (23 October 2019) 133 <https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html>.
[898] Rubinstein (n 893) 1421.
[899] D' Acquisto and others (n 894) 46.
[900] https://www.w3.org/P3P/
[901] Microsoft Internet Explorer and Edge were the only two major browsers supporting this protocol. https://en.wikipedia.org/wiki/P3P#cite_note-3
[902] The EDPS uses PIMs as an umbrella term, encompassing all the other. However other terms are interchangeably used, also depending on the specific technological application used, such as "personal data lockers" or "personal clouds". See, Rebekah Larsen and others, 'Report on Personal Data Stores' (European Commission 2015).http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=10496; European Data Protection Supervisor, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (n 683); European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Thriving Data-Driven Economy' (n 642). I will use the term "personal data stores", "PDS" hereinafter as a

applications or platforms that enable individuals to gather, store, update, correct, analyse, and/or share personal data, according to their preferences. Compared to the other categories of *privacy-friendly* technologies described above, PDSs have a more comprehensive approach in that they aggregate multiple management functionalities into a single platform. In a nutshell, they provide a way for individuals to capture (some of) their data and to obtain granular control over data flowing in/out of the platform, deciding and keeping track of the processing or transfers that may occur, from one single place[903]. Beside this common objective, PDSs may widely differ based on the way they are designed and the underlying business models[904]. They may be based on local storage[905] or cloud-based storage[906]; they may allow only manual input of data into the platform or an automatic retrieval from other sources[907]; data may be processed directly on the user's platform or be securely transferred to requesting third parties. Further, some models may offer anonymity before data disclosure or require specific private or public parties to enter the data ecosystem as intermediate "trust service providers" (e.g., identity providers) to facilitate authorization mechanisms and traceability[908]. Despite structural and technical differences, well-designed PDSs usually provide users with an array of "control management" functions, including effective consent management and privacy preferences mechanisms; user-friendly control dashboards to facilitate the exercise of a number of their subjective rights (such as easy access to their data; keep them up-to-date and request their portability), and enhanced transparency and traceability features[909]. Despite such advantages, the employment of PDS applications for the daily management of data has not yet reached a broad enough audience. However, some PDS projects and tools, both for commercial and research

---

comprehensive term to cover all the tools that allow an overarching management of personal data, rather than stand-alone features of consent or preference management.

[903] Heleen Janssen and others, 'Decentralized Data Processing: Personal Data Stores and the GDPR' (2021) 10 International Data Privacy Law 356, 357.

[904] European Data Protection Supervisor, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (n 896) 6.

[905] E.g. a specific physical device is required in the IoT Databox model, see Janssen and others (n 903) 358.

[906] Online personal cloud solutions are for example CozyCloud, Digi.me and BitsAbout.Me. See Nicolas Anciaux and others, 'Personal Data Management Systems: The Security and Functionality Standpoint' (2019) 80 Information Systems 13, 15.

[907] For example, Cozycloud and Digi.me offer provide their users with a catalog of connectors to retrieve many kinds of personal data (e.g., financial data from banks or PayPal, electricity or telco bills from the respective providers, social network data from Facebook accounts, medical information from hospitals or fitness data from Fitbit), ibid 16.

[908] European Data Protection Supervisor, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (n 896) 7.

[909] ibid 8–11; Anciaux and others (n 906) 27–28; Janssen and others (n 903) 358–361.

purposes, are already developing and available on the market to use. Examples of PDS projects and movements are DataVaults[910], Decode Project[911], PoSeID-on[912] and Solid[913], while existing tools include, among the many others currently on the market Digi.me, HATdex, Mydex or CitizenMe app[914]. In the context of IoT applications, the IoT Databox model has also been strongly promoted as a solution that could offer granular choice and monitoring over data flows between smart devices[915].

The formal endorsement of the Privacy by Design principle and the promising developments of PETs solutions do seem to have great potentials in re-balancing the power dynamics in the data market and provide users with easy and comprehensive tools to regain control over their data. PETs, in their broadest meaning, could effectively alleviate (at least some) important structural challenges that individuals face today as a consequence of the complexities of the new technological context.

2.1.2 Current issues in the effective implementation of privacy-friendly PETs

PDS and other privacy-friendly PETs, however, face a number of issues that substantially reduce their expected impact. A critical challenge for the successful deployment of this technology is the reaching of a critical mass of uptake that stimulates other users and services to endorse PDS[916]. However, currently, these tools have an overarching difficulty to effectively penetrate the market[917]. While privacy-preserving PETs (mostly concerned with reducing identifiability, e.g., cryptographic algorithms, differential privacy, obfuscation techniques and other data masking techniques) have started to gain some traction, it has not been the same for PETs dealing with individual

[910] DataVaults is a EU-funded project under Horizon 2020, that aims to deliver a framework and a platform that collects personal data from diverse sources and that defines trusted and privacy preserving mechanisms allowing individuals to take ownership and control of their data (https://www.datavaults.eu/).
[911] Decode is a Horizon 2020 Programme funded EU project that provides tools that put individual sin control of their data (https://www.decodeproject.eu/). More broadly, the My Data movement promotes initiatives for human-centric data ecosystem (https://mydata.org/). In a similar fashion also the initiatives of the Qiy Foundation (https://www.qiyfoundation.org/).
[912] Another EU-funded project in the Horizon 2020 context, PoSeID-on's goal is to develop a "Privacy Enhancing Dashboard for personal data" to empower data subjects in having a concise, transparent, intelligible and ease access, as well as tracking, control and management of their personal information (https://www.poseidon-h2020.eu/the-project/). See further, Giovanni Maria Riccio and others, 'The POSEID-ON Blockchain-Based Platform Meets the "Right to Be Forgotten"' (2020) 2 Rivista di diritto dei media 194.
[913] Solid is an MIT project led by Tim Burns that proposes set of conventions and tools for building decentralized social applications for true data ownership, https://solid.mit.edu/.
[914] https://digi.me/; https://hatdex.dataswift.io/; https://mydex.org/; https://citizenme.com/.
[915] Lachlan Urquhart, Tom Lodge and Andy Crabtree, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1.
[916] Larsen and others (n 902).
[917] European Data Protection Supervisor, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (n 896) 13–14.

empowerment. This is not only because these types of applications are still in an early-development phase, but also due to the very little incentives for service providers (especially big market players) to switch from the centralized data collection model they currently rely on – where users provide data directly to them, at their terms – to the decentralized version that these technologies would offer. PDS proponents claim that these tools would create a trusted environment where users may be willing to share more data, to the advantage of providers that could benefit from larger data sets[918]. The economic incentive, however, appears too small and uncertain to be attractive for current players, which on the contrary seem to profit mostly from users' inactivity. To shift from a controller-centric to a decentralized and human-centric data management model a more radical cultural change is required. Standardization and technical feasibility are also two further concerns[919]. Absence of commonly agreed standards and interoperable formats slow inevitably down the expansion of the emerging PET industry and risk to create a patchworked framework of different applications that lack the necessary strength to establish themselves on the market. Another open issue relates to the allocation of privacy roles (controller, joint controller and processor) to these new trust intermediaries and the applicable liability regime[920]. There is currently no consistent approach in designating roles and responsibilities: some platforms qualify themselves as "data processor", while others remain silent on the point[921]. Yet to make sure that, from a privacy perspective, decentralized and multiplayers data governance models work properly and to the ultimate benefit of data subjects, a correct allocation of roles and responsibilities is a fundamental aspect.

A final question that may downsize the hype that has been raising around these applications concerns their practical effectiveness in enhancing individual control. On the one hand, in order to maximize their deployment, these technologies are usually addressed to a general public and do not take into account the different cultural backgrounds and variable levels of technical experience of average consumers. As much as these new applications may be designed in a user-friendly manner, whether users have the minimum skillset required to efficiently interact with PETs and makes

[918] Janssen and others (n 903) 362.
[919] European Data Protection Supervisor, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (n 896) 10.
[920] Janssen and others (n 903) 366 ff.
[921] ibid 369.

good use of them remains to be seen[922]. On the other hand, while PDS should provide individuals with easy-to-use data management tools, it is extremely unrealistic to expect that users will be able to manage their data flows with multiple parties from one single device. Yet, if data subjects were to use a number of applications to achieve their control objective, this would inevitably add a layer of complexity that would impair the entire purpose of the solution[923].

2.2 Positive nudges: between legal design and default settings

The issue with "bad" privacy choices largely depends on the cognitive limitations and biases implicit in human nature, that often lead individuals to take decisions that are not rational, free and conscious. These vulnerabilities are exacerbated by the growing complexity of the technological landscape and frequently exploited by data controllers, through dark patterns and other misdirection mechanisms[924], to negatively influence people into disclosing more information or accepting risky data uses to the detriment or in contrast with their privacy interests.

2.2.1 Positive nudges to "gently" guide users towards better choices

Against this background, a growing body of interdisciplinary works has been devoted to researching mechanisms that aim to mitigate these biases or leverage them to the advantage of users, informing and guiding the latter towards safer and better choices[925]. These different interventions are based on and develop the concept coined by Thaler and Sustein of "libertarian" or "soft" paternalism, namely strategies that consciously attempt to «steer people in directions that will promote their welfare»[926], without imposing any particular choice. It stands between the two poles of strong paternalistic approaches (e.g., government regulation) that impose or prohibit certain behaviours that are believed to be beneficial or harmful to users[927], and fully libertarian approaches, where individuals are free to choose how to behave, regardless of the consequences

---

[922] Royal Society (Great Britain), *Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis.* (2019).
[923] Lazaro and Le Métayer (n 31) 33.
[924] Alessandro Acquisti and others, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50 ACM Computing Surveys 1, 25–26.
[925] See broadly in ibid 11 ff.
[926] Cass R Sunstein and Richard H Thaler, 'Libertarian Paternalism Is Not an Oxymoron' (2003) 70 The University of Chicago Law Review 1159, 175 ff. <https://www.jstor.org/stable/1600573> accessed 17 December 2021 see also; Thaler and Sunstein (n 606).
[927] Sunstein and Thaler (n 926) 175 ff. See also the definition in Gerald Dworkin, 'Paternalism' (*The Stanford Encyclopedia of Philosophy*, Fall Edition 2020) <https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=paternalism> accessed 17 December 2021..

that may arise from those behaviours[928]. Soft paternalistic measures, instead, "gently guide" users towards a decision that is supposedly more beneficial for them (thus are not fully libertarian), but preserve users' decisional autonomy, because they do not limit the options users can decide from (thus are not strictly paternalistic)[929]. Libertarian paternalistic interventions are also often referred to as "nudges", defined as «any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives»[930]. Nudging acknowledges that users are affected by a number of cognitive biases, boundaries and routines and uses them to influence individuals into behaving in a certain way, without exerting any form of coercion. While nudges can be exploited to move users away from their interests and closer to those of others (like when companies use dark patterns to manipulate users' behaviour)[931], soft paternalistic approaches assume that nudges are positively leveraged to lead users to more beneficial outcomes, therefore to make decisions that are better aligned with their privacy interests[932]. They are aimed at improving the background against which people make their decisions.

Soft paternalistic interventions have been differently employed as policy instruments in a variety of fields (e.g., warning images on cigarette packages or eye-catching nutrition labels on unhealthy foods), with the intent to promote citizens' welfare without excessively curtailing their freedom of choices[933]. Because of their both libertarian and protective characteristics, they seem appealing for the data protection context. These measures ultimately preserve a sphere of individual control over decisions that data subjects make with regard to the processing of their personal data; at the same time, they shield them from influences that may negatively affect them during the decision process. In this sense, "positive" nudges might be a workable middle ground between privacy self-management and strict regulation[934].

---

[928] Sunstein and Thaler (n 926) 175.
[929] ibid; Pelle Guldborg Hansen, 'The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?' (2016) 7 European Journal of Risk Regulation 155, 159.
[930] Thaler and Sunstein (n 606) 6.
[931] On the use of "nudging" by controllers, see Chapter II above.
[932] Hansen (n 929) 158 ff.
[933] On nudging smokers see Alberto Alemanno, 'Nudging Smokers The Behavioural Turn of Tobacco Risk Regulation' (2012) 3 European Journal of Risk Regulation 32 on nusging for healthy eating see; Gyorgy Scrinis and Christine Parker, 'Front-of-Pack Food Labeling and the Politics of Nutritional Nudges: Front-of-Pack Food Labeling' (2016) 38 Law & Policy 234 for a general overview see also ; Acquisti and others (n 924) 13 ff. ibid 13 ff.
[934] Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1901.

Nudges proposed in the privacy context consist in a wide spectrum of interventions that vary greatly in terms of the *type* of mechanism used to exert influence and the *level* of influence that it is exerted on the actions and behaviours of individuals[935]. For example, measures that focus on increasing transparency, that play essentially on information presentation, have a more limited impact on data subjects' privacy decisions than the implementation of default setting.

PRIVACY INFORMATION PRESENTATION - Abundance of information is often a critical issue for data subjects. In a datafied society where data processing are ubiquitous, GDPR transparency requirements produce daily storms of lengthy privacy notices that make individuals feel overwhelmed, uninformed and, ultimately, lost. In many instances, the hurdles individuals experience when faced with privacy decisions have to do with *how relevant information is presented* to them. Numerous studies, both in and outside the privacy context, have shown the powerful effects of "presentation components" on human perception and understanding. Framing information using a certain language or ordering it in a certain manner can impact users' behaviours, increasing their perception of saliency for certain elements (e.g., risks, damages, consequences) and directing their focus on certain information rather than others.

With the data protection reform, the importance of communication and presentation aspects of privacy notices for achieving effective transparency has been formally recognized in the GDPR. Beside listing privacy notices' substantial contents (Articles 13-14 GDPR), the regulation has included also general indications on the presentation of privacy information to users in a «concise, transparent, intelligible and easily accessible form, using clear and plain language»[936]. Soft law interventions of the WP29 have contributed to give practical meaning to the GDPR principle of transparency, providing "good" and "bad" examples of privacy notices' drafting techniques[937].

The growing attention to the power of visualization and design of legal information has more recently found expression under the newly developed interdisciplinary domain of "legal design"[938]. Legal design is a general concept that refers to the application of

[935] Acquisti and others (n 924) 12.
[936] Art. 12 of the GDPR.
[937] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (29 November 2017) WP260 rev.01.
[938] The term "legal design" was coined by Margaret Hagen, *Law by Design* (2018) <https://lawbydesign.co/>.

«human-centered design to the world of law»[939], therefore promote the design and drafting of legal documents (such as privacy notices) in a human-centered and usable way that takes into account the perspective of its users (i.e., data subjects)[940]. The legal design approach is usually portrayed in neutral terms, with no specific nudging objective. However, since any "choice of architecture" in some way entails a form of nudging[941], the measures applied by legal design in the construction of data subject-friendly privacy notices are in fact addressed to guide users' perception and attention, thus influencing their subsequent conduct.

Legal design strategies include a range of mechanisms that variously apply to the graphical, linguistic and/or structural components of privacy notices[942]. These include, for example, the inclusion in privacy notices of practical examples to make legal terms or abstract concepts more tangible; or the provision of short summaries and easy-to-consult FAQs concerning the most difficult clauses or important legal topics, all of which may play a significant role in mitigating comprehensibility issues linked to language complexity and excessive length of privacy notices[943]. Further, the choice of the correct wording (tailored to the targeted audience)[944], the distribution of information on different layers that contain increasingly detailed explanations (so called "layered notice")[945] and the structured organization of the policy in a coherent manner, distinguishing information by theme and hierarchy[946], have also proven to be efficient tricks to focus users' attention on a limited number of essential information and prevent them from feeling overwhelmed. One of the most discussed and appreciated strategies to convey privacy information, acknowledged by both the WP29[947] and supervisory authorities[948],

[939] Margaret Hagen, *Legal Design* (2018) <https://lawbydesign.co/>. See also Rossana Ducato and others, 'Legal Design Manifest' <https://www.legaldesignalliance.org/>.
[940] Born mainly from contract and information visualization, the concept of "legal design" has expanded to cover also the process of designing and prototyping legal artefacts, services, organizations, and systems.
[941] According to Thale and Sustein, any "choice architecture" (design of information), whether intentionally designed to affect users' behavior or not, will impact how users interact with a system. Thaler and Sunstein (n 606). In the same way, Acquisti et al. argue that most user design interfaces can be viewed as nudges of some kind, Acquisti and others (n 924) 27.
[942] Helena Haapio and others, 'Legal Design Patterns for Privacy' in Erich Schweighofer and others (eds), *Data protection/LegalTech: proceedings of the 21st International Legal Informatics Symposium* (Editions Weblaw 2018).
[943] Arianna Rossi and others, 'When Design Met Law: Design Patterns for Information Transparency' [2019] Droit de la Consommation 98–107.
[944] ibid.
[945] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 937) 19.
[946] See https://legaltechdesign.com/communication-design/portfolio-item/structured-layout/ .
[947] Article 29 Data Protection Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 937) 25.

involves the use of non-textual signs (like graphic components or self-explanatory icons)[949] or alternative visual materials (cartoon images or audio-video messages)[950] that simplify the user experience and boost users' motivation. These different strategies can be coupled with additional measures that provide users with an interactive experience. Sending users periodic feedbacks concerning how online activities are tracked or reminders on the type of data that users are sharing[951] have been used to increase users' awareness over time. Similarly, the development of gamified experiences to convey privacy information[952] and the introduction of "visceral" notices, that draws from consumers' experience of a product or service to warn or inform[953], may help to overcome information asymmetries and transaction costs of traditional notices, making users converge towards privacy settings that are better aligned with their preferences.

PRIVACY CHOICES DESIGN - Behaviours can be nudged not only by affecting the users' understanding of a certain activity, based on how essential information on the activity is presented, but also by altering how privacy choices (e.g., opt-in and opt-out options; privacy settings) are designed and submitted to users. Studies on cookies have shown how the choice of architecture in cookie banners can significantly induce users to share more data[954]. The use of colours (green and red) and dimensions to entice users to click or not to click a "consent" button or the framing of privacy choices with a positive or negative language are also different tactics that can be employed to nudge users towards a preferred option[955]. The same effect can be achieved by providing options in a certain order or structure. In complex decisional contexts, a careful design of the

[948] See for example the initiatives of the Italian DPA: Garante per la protezione dei dati personali, 'Semplificare Le Informative Privacy Attraverso Il Metodo "Creative Commons". Protocollo Tra Garante Privacy e Creative Commons' (2021) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9684797> accessed 18 December 2021; Garante per la protezione dei dati personali, 'HACKtheDOC: il primo hackathon italiano di legal design. Il Garante per la protezione dei dati personali propone la challenge "Infoprivacy"' (2020) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9500152> accessed 18 December 2021.

[949] Arianna Rossi and Monica Palmirani, 'Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection' (2020) 36 Design Issues 82.

[950] Haapio and others (n 942).

[951] Acquisti and others (n 924) 17.

[952] Rossi and others (n 943) 118.

[953] Calo (n 570).

[954] Jan M Bauer, Regitze Bergstrøm and Rune Foss-Madsen, 'Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data' (2021) 120 Computers in Human Behavior 106729.

[955] Information Commissioner's Office (ICO), 'Nudge Techniques' (14 October 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/> accessed 18 December 2021.

privacy choices' architecture can mitigate the effects of mental shortcuts and availability heuristics, and assist users in making decisions that are more beneficial for them[956].

DEFAULT SETTINGS or INCENTIVES - Strategies that have a more impactful nudging effect on individuals leverage certain human biases to avoid or prompt certain actions.

Some authors, for example, have emphasized the potential of default settings that take advantage of individuals' tendency to stick with given choices rather than activate to make their own[957]. Privacy-friendly default settings (e.g., blocks by default on certain data uses or data sharing) can be employed to serve individual privacy expectations, particularly in complex decision-making scenarios in which it is unreasonable to assume that users are able to make an optimal choice[958]. Browsers' "Do Not Track" (DNT) default options, which prevent by default tracking cookies from being installed on users' devices, bypassing the mass of cookie banners set up by websites, are a typical example of how this approach can be used to the advantage of online users. DNT default settings have been adopted by a few browsers that have started to enable them in their systems[959] and have been the object of debate during the discussions of the e-privacy Regulation. These type of "mass" defaults could be mandated to protect conventional users, while still allowing expert users to customize data sharing and uses according to their needs. As an alternative to general defaults, that apply indifferently to all individuals, some authors have argued in favour of "personalized default settings that, although require an initial processing of data to tailor the setting to the specific user, are in the end more respectful of each one's needs[960].

Like defaults, another strong nudge to direct users towards a specific configuration could be the introduction of specific non-financial "incentives" to privacy choices, either in the forms of punishment/costs or in terms of rewards. Behavioural studies have shown how incentives can use the loss aversion bias to create short-term disadvantages or advantages to induce users to take a particular decision[961]. In a privacy context, where privacy harms are abstract and long-term, thus are often not

[956] Acquisti and others (n 924) 19.
[957] For an overview see Athina Ioannou and others, 'Privacy Nudges for Disclosure of Personal Information: A Systematic Literature Review and Meta-Analysis' (2021) 16 PLOS ONE <https://dx.plos.org/10.1371/journal.pone.0256822> accessed 18 December 2021.
[958] ibid.
[959] Alfred Ng, 'We Need to Talk about Default Settings for Privacy' (*CNET*, 21 December 2019) <https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/> accessed 18 December 2021.
[960] Acquisti and others (n 924) 21.
[961] See contributions quoted in Ioannou and others (n 957) par. 3.3.4.

perceived as imminent "losses", the introduction of more practical and short-term costs (e.g., increasing the cost or difficulty in making riskier privacy choices or configurations) may help to re-balance users' cost-benefit analysis. On the other hand, secure or less risky configurations can be made easier to select, encouraging users to opt for them[962].

2.2.2 Concerns in the application of positive nudges

Trust in the power of nudges to guide individuals into making "good" privacy choices faces a number of issues on the opportunity of nudging and its effectiveness.

A first point concerns the direction that a positive privacy nudge should take. Nudging assumes that a particular entity (policy maker or system designer) is better positioned to decide what choice the individual should make[963]. Therefore, it requires these entities to make a decision in favour of a nudge in a particular direction[964], which is deemed to be best for individuals or society at large. What criteria should be used to measure this "benefit" however is not that easy to determine, particularly when it comes to privacy decisions, given that privacy harms are often long-term, intangible or difficult to measure[965].

Who should design and implement these nudges is a further point of discussion. In the absence of adequate market forces that could drive companies to implement user-friendly nudges, regulatory approaches that mandate companies to implement certain nudges could be a more appropriate solution[966]. However, lacking proper supervision, delegating to companies (thus controllers) the responsibility to execute and secure these mechanisms to the best interest of users raises some concerns. Also, the resilience of legally-imposed design choices and defaults would be made more difficult by the speed of technological changes, that could render them ineffective within a short period of time[967].

Finally, nudges have been questioned also in terms of their effectiveness to actually improve individuals' decision-making[968]. Changes in privacy notices' design and

[962] Acquisti and others (n 924) 22.
[963] ibid 28.
[964] Eoin Carolan, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32 Computer Law & Security Review 462, 472.
[965] Acquisti and others (n 924) 28.
[966] ibid 29.
[967] Carolan (n 964) 472.
[968] Ilaria Amelia Caggiano, 'Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo(GDPR) e analisi comportamentale. Iniziali spunti di riflessione' [2017] Diritto Mercato Tecnologia 13 <https://www.dimt.it/la-rivista/articoli/il-consenso-al-trattamento-dei-dati-personali-tra-nuovo-

communication have in fact contributed only to marginal improvements in individual decision-making abilities[969]. Further, since the foundational logic of nudging is that individuals are subjects to subconscious cognitive biases, it has also been argued that faith in minimalistic nudges can be perceived at least as delusive, as the reliance the GDPR currently place on "free" consent[970].

3 Legal measures

With a view to strengthen individual oversight powers, the GDPR placed great emphasis on data subject's rights, extending and clarifying their original scope or introducing new ones. These rights, some more than others (e.g., right to access, to data portability, right not to be subject to automated decision-making), have been praised for their renewed ability to provide individuals with better instruments to fight against the dangers of hidden misuses, manipulations and unlawful dissemination of their personal information. None of these rights is, however, immune from the technological and legal challenges, briefly explored in the previous chapter, which substantially curb their practical effectiveness.

To overcome some of the failures experienced by existing rights and supplement the range of tools that data subjects may benefit from for a genuine exercise of control, scholars have suggested various solutions, that have not yet found formalization in legal norms, and have proposed an expansive interpretation of current rules, which however still lack explicit endorsement by national DPAs' or EU Courts.

3.1 Recognizing a "right to property" on personal data

Arguments in support of the introduction of property rights in personal data have received considerable attention, particularly in the US, starting from the 1970's, and, even if not with the same impetus, the debate on the propertization of personal data has reached also the European continent.

In recent years, the issue of ownership in personal data has gained new traction. The undeniable recognition of the growing economic value of data[971] and the emergence of

---

regolamento-europeo-gdpr-e-analisi-comportamentale-iniziali-spunti-di-riflessione/> accessed 19 December 2021.

[969] E.g., in Calo (n 570) 1033; Omri Ben-Shahar and Adam Chilton, 'Simplification of Privacy Disclosures: An Experimental Test' (2016) 45 The Journal of Legal Studies S41.

[970] Carolan (n 964) 472.

[971] See e.g., European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Thriving Data-Driven Economy' (n 642); European Commission, 'Communication from the Commission

the B2B data market, the deployment of applications that allow users to gain compensation for sharing certain data with service providers[972], the occasional references made by EU representatives that «we own our data»[973] or that data could be treated as counterperformance[974] have encouraged the idea that individuals may in fact assert some proprietary rights on their information. Decisions of national courts or authorities, that have indirectly accepted such possibility[975], have further reinforced this property thinking.

Traditionally, EU positions have been sceptical towards the idea of considering personal data an object of property, on the basis that data protection is a self-standing fundamental right of individuals (Art. 8 EU Charter), devoted to the protection of particular aspects of their individuality and personality. From the conception of fundamental rights as closely linked to constituting and maintaining a person's personal integrity and development[976], it has been argued that these rights were, by their very nature, non-commodifiable[977]. Hence, a regime introducing a property right on personal data, resulting in the possibility for individuals to "trade-off" data protection in exchange of economic gain was generally interpreted as a commodification of the individual

---

to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building A European Data Economy' (n 643).

[972] E.g., personal data stores such as CitizenMe, that allow users to obtain an instant "cash reward" when they share their data with businesses, https://citizenme.com .

[973] For example, during an interview, the European Competition Commissioner Margrethe Vestager expressly said: «Because now we know that we all own our data. But the thing is that we give very often a royalty-free license for the big companies to use our data almost to whatever. So, for smaller businesses to get access to huge amounts of data, to be able to innovate, to be able to provide services, how can we enable us to give this access since we now own the data?». 'Vestager on the Intersection of Data and Competition' *IAPP* (30 October 2018) <https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/> accessed 5 July 2021.

[974] The reference was initially included in 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 ("Digital Content Directive"). It was later removed after consultations with the EDPB, which strongly advised against it.

[975] See for example, the Austrian DPA decision of 30 November 2018 on cookie consent (the DPA essentially stated that an online newspaper could ask their readers to either pay a small fee to subscribe to the newspaper or consent to the processing of their data to access a specific article, thus implicitly qualifying personal data as a counterperformance) available at https://iapp.org/news/a/austrian-dpa-provides-favorable-decision-to-online-news-outlets/; Italian Supreme Court decision n. 17278/2018 (similarly to the Austrian DPA, the Court accepted that the access to a service could be subject to the consent of the user to process his data – not strictly necessary for the provision of the service itself – provided that similar alternative services were available in the market); the Italian Antitrust Authority (AGCM) decision n. 27432/2018 (the authority concluded that Facebook Ireland Ltd. and its parent company Facebook Inc violated the Italian Consumer Code for misleading practice, since the companies had emphasized the "free" nature of their service, whereas users' personal data were used for commercial purpose).

[976] Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of Our Identity' (2006) 15 Information Law Series 223, 234.

[977] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 241; Prins (n 976) 234.

himself, which contrasted with EU human rights-based system of data protection[978]. Opposing these views, other scholars have argued that nothing in the EU legal framework would prevent the introduction of a property regime on personal data, neither the fundamental right nature of data protection[979], nor its strict connection with personality traits[980]. On the contrary, some have argued that both the DPD, and now the GDPR do already envisage instruments of control and power that may be assimilated to property-like rights[981].

Despite on-going lively discussions, to date, there has been no formal recognition, nor legal establishment of a property regime on personal data.

Yet, leaving aside the feasibility and compatibility issues, the debate on the propertization of personal data has a specific interest for the purposes of our analysis, since, among the reasons put forward in favour of the formal establishment or

[978] Prins (n 976) 235. See also the European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (14 March 2017). In its opinion the EDPS affirms in particular that «one cannot monetise and subject to a simply commercial transaction a fundamental right».

[979] Some authors point out the non-absolute character of the fundamental right to data protection, that should be legitimately balanced against other fundamental rights, including those protecting economic-driven interests, such as freedom to conduct business. Vincenzo Ricciuto, 'La Patrimonializzazione Dei Dati Personali. Contratto e Mercato Nella Ricostruzione Del Fenomeno' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (2019). Others argue that the fundamental right nature of the right to data protection does not *per se* precludes a commodification of personal data, but serves as outer boundary to its tradability. In particular, according to Purtova «data protection guarantees which enjoy human rights protection cannot be freely contracted around or waived, and the ambit of the permitted contractual or property rights is limited by the existing basis of the data protection rules». Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2012) 222. A more extreme view, that favours a prevalence of the fundamental right of freedom of contract to "contract around" the limitations of the EU data protection regime (that would remain applicable only when no contract governs data processing situations), see Colette Cuijpers, 'A Private Law Approach to Privacy; Mandatory Law Obliged?' (2007) 4 SCRIPT-ed 304, 306 ff.

[980] In this sense, different authors have underlined the growing acceptance of the merchantability of certain attributes of individuals' personality (person's name, appearance, voice or likeness), that would confirm an openness towards the exploitation of some forms of incorporeal aspects of personal identity, provided they are subject to a special tradability regime that provides a minimum standard of protection.
For a critical look on the extra-patrimonial and inalienable nature of personality rights. Giorgio Resta, 'The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives' (2011) 26 Tulane European and Civil Law Forum 33.

[981] Purtova, *Property Rights in Personal Data* (n 979) 193–202. She argues that nothing in the DPD prohibits or excludes introducing property rights in personal data, particularly since individual rights of control (common denominator of all proprietary regimes) are already provided for by the DPD. Propertization, however, should be confined within the limits established *inter alia* by the DPD itself (i.e., freedom of contract cannot be invoked to waive established data subject's rights). See also Prins (n 976). Prins is generally opposed to the idea of vesting personal data with property rights, but acknowledges that some instruments of control and power are included in the DPD regime and «some may thus claim that, at least in a commercial setting, a property approach may not be such a very strange phenomenon under the European regime». With the adoption of the GDPR, some authors contend that GDPR rules introduced some property-like rights, pushing the propertization approach of the DPD even further, e.g. Victor M Jacob, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 The Yale Journal 513.

recognition of a property regime on personal data and the qualification of data subjects as "owners" of their data, an often-quoted motive concerns its potentiality in enhancing the control individuals could exert on their data.

Relying on economic argumentations, dominant particularly in the US debate, authors have argued in favour of a propertization regime, as a mean to provide individuals with maximum control over their information, which would in turn maximize utility and achieve efficiency of the "information privacy" market[982]. The introduction of a property right would in fact enable data subjects to adapt their data processing preferences to the value they individually give to different data processing situations[983], thus enabling them to choose their "preferred level" of privacy. Other authors have instead claimed that a formal recognition of a property regime would also increase individuals' perception that data have an intrinsic value worth protecting, and would create adequate incentives for data subjects to better monitor and manage the sharing and use of their personal data, *de facto* reinforcing the control they exercise, and, according to these authors, the overall level of protection[984]. On a similar vein, scholars have also argued that turning a blind eye on the tradability of personal data, which willing or not is a consolidated reality, perpetuates only a double standards, based on which companies consider themselves as "owners" of the data set they collect and are able to exploit and sell it for profit, whereas data subjects are deprived of the possibility to exert this type of "ownership" and are thus left in an weaker position[985], as they have no contractual power to contrast possible abuses.

3.1.1 A proposal for a property right based system in the EU

The US scholarly debate on the propertization of personal data has produced a number of proposals suggesting how a property regime on personal information may work in practice[986], which are however tailored to the specificities of the US legal system. The EU landscape has been traditionally more cautious. One of the most comprehensive

[982] For a comprehensive overview of the economic arguments for propertization in the US debate, see Purtova, *Property Rights in Personal Data* (n 979) 133–140.
[983] See from the US perspective Lawrence Lessig, 'Privacy as Property' (2002) 69 Social Research: An International Quarterly 247, 225. From the EU perspective, Cuijpers (n 979) 315.
[984] See in the US literature, Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056; Lessig, 'Privacy as Property' (n 983); Pamela Samuelson, 'Privacy As Intellectual Property?' (2000) 52 Stanford Law Review 1125. In the EU literature, see in particular Purtova, *Property Rights in Personal Data* (n 979).
[985] See e.g. Ricciuto (n 979).
[986] Schwartz, 'Property, Privacy, and Personal Data' (n 984); Samuelson (n 984); Lessig, 'Privacy as Property' (n 983).

explorations on the benefits (in terms of "enhanced individual control") of a property regime in the EU framework and on how its practical construction may look like in practice has been presented by Purtova[987]. To construe her analysis with the broadest possible scope and prevent it from being invalidated by national peculiarities, as a preliminary step, the author clarifies the meaning assigned to the notion of "property rights"[988]. In doing so, she identifies as common denominator of property rights across European legal systems their *erga omnes* effect, namely the possibility for these rights to be enforced against the world[989], which is strictly linked to two further leading principles of property law: the *numerus clausus* principle (the rights need to be recognized by law) and the transparency principle (the rights need to be made public to be enforceable against third parties)[990]. Following these conclusions, Purtova argues that it is the *erga omnes* effect that characterizes property rights that makes them a suitable legal instrument to achieve a stronger individual control over personal data. This effect, supported by the establishment of a transparent framework for the management and exchange of personal data, would in fact enable data subjects to enforce their control powers against any entity in the chain of exchange coming in contact with their data[991]. This form of "control against the world" is claimed to be especially useful in the complex conditions of the modern data flows, where location of data and the chain of control over it are hard to trace to known contract parties[992]. According to the author, the institution of this new property-based system would develop on two foundational blocks: a) the establishment of default control rights of data subjects (i.e., the "consent rule" should become a default condition of legitimate data processing); and b) the creation of a "leases scheme" in personal data, resembling the

[987] Purtova, *Property Rights in Personal Data* (n 979).
[988] "Property rights" refer to the entire catalogue of "real rights" or "rights in *rem*", thus including full title of property and "minor" real rights. Correctly, Purtova points out that many of the issues when discussing about property rights in personal data stem from the lack of a common understanding on the concept of "property". On the one hand, the notion is used differently in the legal and economic fields. On the other hand, in the EU framework, the concept of "property" has very flexible meanings and requirements from national legal system to legal system. Clarifying the definition of property is therefore a necessary pre-requisite before entering in the discussion of property rights in personal data.
[989] Purtova, *Property Rights in Personal Data* (n 979) 80–85. She reaches these conclusions drawing from Van Erp's comparative study of property law across Europe. Sjef JHM van Erp, 'From "classical" to Modern European Property Law' in Konstantinos D Kerameus (ed), *Essays in honour of Konstantinos D. Kerameus* (Ant N Sakkoulas ; Bruylant 2009).
[990] Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (n 719) 67. More extensively Purtova, *Property Rights in Personal Data* (n 979) 83–84.
[991] Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (n 719) 68.
[992] ibid.

property right regime of land[993]. In practice, data subjects would be granted the broadest property right possible on their personal data (including the right to transfer data for remuneration)[994]. However, in view of the fundamental right nature that the right to personal data enjoys in the EU, the right to property would be limited by law to prevent individuals from completely waiving existing data protection guarantees[995], thus they could not entirely relinquish the control over their personal data. This would leave individuals with the possibility to transfer "bits" of property rights in personal data (i.e., a closed list of minor property rights), which would take the form of "leases" in personal data that could be further transferred to other subjects under the same or stricter conditions[996]. The transferable personal data "leases" could be tailored to reflect most common uses of personal data, and could vary in type (depending on the characteristics of the processing and on its limitations, e.g., excluding the use of the data for profiling)[997]. The original owner (i.e., the data subject) would still maintain some control even when his data is transferred to an undefined number of transferees along the chain since the *erga omnes* protection, conferred by his property right, would ensure the same degree of accountability for every actor involved in the data processing chain[998]. Such a leases' scheme would be subject to specific transparency and traceability requirements (that could be implemented through the use of sticky technologies), that would further help to maintain under track the occurred data transfers, therefore the chain of involved actors. As a result, according to Purtova, this system proves the protective potential of individual property rights in personal data in providing individuals with effective legal tools facilitating individual control over collection and use of their data[999].

[993] Purtova draws inspiration from English land law, where "leases", that allow full owners to share the use and enjoyment of land, counts as a property right that binds third parties even if a freehold changes hands. This would be somewhat similar to the *ususfructus* or *usus* real rights under civil law systems.
[994] The author focuses on the transfer of property rights by contract as the main transfer mechanism and does not further deal with the other possible ways of acquisition of property available under national legal systems.
[995] Purtova, *Property Rights in Personal Data* (n 979) 249–250. This property regime resembles the highly regulated property regimes proposed by US scholars such as Schwartz (n 305); and Janger (n 308).
[996] Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (n 719) 68.
[997] ibid.
[998] Purtova, *Property Rights in Personal Data* (n 979) 250–255.
[999] Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (n 719) 68.

3.1.2 Doubts on the effectiveness of propertization to enhance individual control

Beside criticisms highlighting the overly-costly implementation of a property-based leases system[1000], such as the one envisaged by Purtova, other critical remarks have been moved against the idea that the propertization of personal data could bring practical improvements in individuals' ability to control their data.

A first argument focuses on the complex technological context in which data subjects would be expected to exercise their property rights. The scale of data processing would make it, in fact, materially impossible for data subjects to micro-manage in their day-to-day practice their preferences[1001], irrespective of the economic incentive and more intense control powers the new framework provides them with. A regime that aims at placing individual choice at its core risks to backfire on data subjects, leaving them even more isolated and burdened to self-manage their privacy preferences for each data processing situation. This would result in a system with stronger forms of individual control, on paper, but the same shortcomings of the current data protection model, in practice.

Formally recognizing a right to property on personal data would also hardly disrupt existing business practices, that tend towards a standardization of terms and conditions, rather than their customization[1002]. Data subjects would thus not be freer to determine and negotiate the terms of their transfers, rather would be even more exposed to the power dynamics already existing in current business-consumer relationship. The weaker position of data subjects would be further confirmed by the fact that information asymmetries and bounded rationality issues would certainly not disappear under a property right approach[1003]. The opportunity for short-term financial gains may also distort individuals' perception and make them more easily manipulated, diverting them from considering the possible long-term risks of certain data uses in favour of immediate economic advantages that the data transaction may offer them[1004].

Finally, other authors have underlined how the establishment of a hyper-individualistic regime, such as the property one, would further exacerbate the negative impacts that

[1000] Prins (n 976) 251 ff.
[1001] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 247.
[1002] Prins (n 976) 246.
[1003] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 248–250.
[1004] According to Kang framing the data protection issue as a property right issue may lead people to «treat their personal data like their car» Jerry Kang and Benedikt Buchner, 'Privacy in Atlantis' (2004) 18 Harvard Journal of Law & Technology. 230; quoted in Lynskey (n 327) 238.

the atomistic behaviour of individuals, strengthened in this case also by personal economic interests, may have on collective and social interests[1005].

In brief, should a propertization regime on personal data be formally introduced or recognized and individuals be legitimized to transfer their data in exchange of financial gains of any sort, while it may help to improve the transparency and (more hardly) traceability of data transfer and uses, it is questionable that this new framework could actually solve the substantial shortcomings that the current non-proprietary individual control approach suffers.

3.2 Recognizing a "right to explanation" of automated decision making

In the presence of automated decision-making processes, the GDPR imposes certain information obligations on controllers, which include the provision of meaningful information about the *logic* involved, as well as the *significance* and the *envisaged consequences* of such processing for the data subject (see Art. 13(2)(f); Art. 14 (2)(g); Art. 15(1)(h) GDPR). As previously mentioned, these information requirements have been generally interpreted, and applied in practice, as obligations for controllers to provide individuals with elements describing the "system functionality", in general and abstract terms, such as its pre-determined logic and envisaged consequences[1006] (i.e., "Model-Centric Explanations", MCEs[1007], namely information that focus on how the machine should construe and apply the decisional model).

Against this reading, however, some scholars started to suggest that the GDPR had in fact introduced a "right to explanation"[1008] of automated algorithmic decisions, namely a right to obtain clarifications not simply covering a description of the general functioning of the system, rather an illustration of the specific and personalized mechanisms underlying the case-by-case decision originating from the automated process. This means providing not simply generalized elements on the abstract logic of the algorithm, but the specific rationale and the individual circumstances considered in the decision-

[1005] Lynskey, *The Foundations of EU Data Protection Law* (n 44) 246.
[1006] Wachter, Mittelstadt and Floridi (n 773) 3.
[1007] In computer science terminology, this type of explanations focused on the general machine functioning have been referred to as "Model-centric Explanations". MCE can include a varied set of information, even very technical in nature, such as (i) the intention behind the modelling process; (ii) the parameter and metadata used to train the model; (iii) information on the model predictive skills, (iv) information on how the model was tested, trained and screen. 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, 55.
[1008] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 AI Magazine 50.

making process[1009] (i.e., "Subject-Centric Explanations" or SCEs[1010]). As a consequence, this type of explanation could be provided only *ex-post*, meaning after the data processing and the decision has taken place, being it strictly connected with the outcomes of the specific decision process. It is argued, in fact, that only by recognizing a right to explanation of this sort, individuals could be empowered, as they would be provided with the necessary elements to effectively monitor and exert some influence over data processing that directly impact them. Through practical and *ad hoc* explanations, individuals would in fact be able to understand more clearly why a specific decision concerning them is adopted and would have better grounds to challenge and express their point of view on adverse decisions[1011], or understand what could be changed to obtain a desired result in the future[1012].

3.2.1 Does a right to explanation already exist?

Despite most scholars agree on the overall advantages of a broadly interpreted right to explanation, a fierce debate has developed around the existence or not in the current framework of sufficient legal grounds to claim its application. Some argue the GDPR did not create any legally binding "right to explanation" and, should it be deemed a suited safeguard, it would have to be formally introduced[1013]; others, on the contrary, claim that a right to receive an *ad hoc* explanation can already be inferred from the wording of the norms on automated decision-making processes[1014]. Finally, there are authors who, despite acknowledging the possibility of implementing a right to explanation, criticize its practical effectiveness[1015].

[1009] Wachter, Mittelstadt and Floridi (n 773) 3.
[1010] Edwards and Veale (n 1007) 56. Veale and others distinguish among four types of SCEs, that help to provide individuals with understandable information in the form of answers to specific questions concerning the decision, namely (i) sensitivity-based (what changes in my input data would have made my decision turn out otherwise?); (ii) case-based which data records used to train this model are most similar to mine?); (iii) demographic-based (what are the characteristics of individuals who received similar treatment to me?); and (iv) performance-based (how confident are you of my outcome?).
[1011] Brkan (n 763) 114.
[1012] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841, 842.
[1013] Wachter, Mittelstadt and Floridi (n 130) 81 and footnote 66 point out that the text of art 22 GDPR has not been changed much compared to art 15 of the Data Protection Directive; see also; Giusella Finocchiaro, 'Intelligenza Artificiale e Diritto - Intelligenza Artificiale e Protezione Dei Dati Personali' (2019) 7 Giurisprudenza Italiana 1657.
[1014] Mendoza and Bygrave (n 793) 7; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233, 237; Brkan (n 763) 111–112.
[1015] Edwards and Veale (n 131) 44 ff..

Scholars, who claim that only an *ex-ante* and general "right to information" exist, build their arguments on a literal and contextual interpretation of GDPR articles. The central observation is that a right to explanation is only explicitly mentioned in the non-legally binding Recital 71 of the GDPR[1016] and not in the main body of the law, particularly not under Art. 22 GDPR, which specifically deals with automated-decision making[1017]. An omission that, according to these authors, seems to be intentional, as confirmed by the fact that the inclusion of a binding right to explanation in the early drafts of Art. 22 was eventually dropped in the final text[1018]. The right would not easily fit neither under Articles 13(2)f nor 14(2)g GDPR, because the language used in those articles ("logic" and "envisaged consequences") and the timing of the notification duties (*before* the data processing/decision is made)[1019] appear to validate the interpretation that only an *ex-ante* functional explanation is required[1020]. Scholars supporting this view acknowledge that the "right to access" recognizes data subjects also the right to receive meaningful information about the logic involved, after the processing has taken place ("upon their request"), therefore may be a stronger basis to claim the introduction of an obligation to provide an *ex-post* explanation. However, they still conclude it is more coherent to read the norm as imposing only an information duty regarding the *system functionality*, consistently with the evolution of the right to access under the DPD[1021]. Lacking a solid legal basis in the GDPR, a meaningful right to explanation should be introduced, where deemed appropriate, as an additional right, either amending the text of the law (considered unfeasible) or via express judicial validation (more plausible)[1022].

Opposing these positions, a different group of authors challenges a strict reading of GDPR rules and advocates for a systematic and purposeful interpretation of the data

[1016] Recital 71 GDPR : «[…] In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to *obtain an explanation of the decision* reached after such assessment and to challenge the decision. […]»
[1017] The 2012 EC's proposed text did not contain a right to explanation. The European Parliament proposed an amendment to Art. 20 to strengthen the safeguards included against automated decision-making, introducing also a "right to obtain an explanation". The suggestion was not taken up by the European Council, which suggested as a compromise solution to include the wording only in the recital section, as it was eventually agreed in the final text. Wachter, Mittelstadt and Floridi (n 773) 4–5.
[1018] ibid 5–6.
[1019] Also the authors recognize that the affirmation did not fit perfectly under Art. 14 GDPR (i.e., personal data collected from third-parties), where the privacy notice is required at the latest within a month from collection or at the time of first communication with the data subject or first disclosure to a third-party, all situations in which the data processing may have been already started.
[1020] Wachter, Mittelstadt and Floridi (n 773) 8.
[1021] ibid 9.
[1022] ibid 16.

protection framework, that allows a right to explanation to be inferred from existing subjective rights. Regardless of the name with which this right is called in different works (e.g., "explanation"[1023] or "to be informed about the reasons for the automated decision"[1024]), what does not change is the content this right needs to convey: the understanding of the rationale of a specific decision, beyond the assurance of a "procedural regulatory" in its formation[1025]. Looking at the grounding legal norms of a right to explanation, the majority of scholars affirm that the right to explanation should be derived from one or a combination of Articles 13, 14 and 15 GDPR[1026] or, more broadly, from a holistic interpretation of the GDPR, which includes also Recital 71 and Art. 22[1027]. The argumentations put forward to defend this thesis follow largely the same lines. The "timing problem" raised by the opponents of a right to explanation is easily dismissed on the basis that the claim may be valid for Art. 13, but finds no sufficient grip in Articles 14 and 15, whose forward-looking wording or lack of specification on the timing at which the "meaningful information" needs to be communicated do not exclude, on the contrary suggest, that the underlying intent was to provide individuals with information on the specific decision after it was taken[1028]. The claim that the right does not exist because the only express mention is contained in Recital 71, with no binding nature, is also disregarded for being too formalistic, especially in light of CJEU case-law[1029], which proves that recitals are commonly treated as very valuable interpretative aids. Further reasons advanced in support of a right to an *ad hoc* explanation concern the instrumental nature of this right as a necessary pre-condition for the full exercise of the other safeguards established by Art. 22(3) (e.g., to express a point of view and to contest the decision), without which they would remain empty formulas[1030]. The latter interpretation would be backed by the open wording of the same paragraph that emphasizes the non-exhaustive nature of the safeguards listed, suggesting that there is room for the adoption of additional measures[1031]. A teleological interpretation of the

[1023] Goodman and Flaxman (n 1008); Selbst and Powles (n 1014); Mendoza and Bygrave (n 793).
[1024] Brkan (n 763) 113.
[1025] "Procedural regularity" ensures that a decision has been taken following a pre-established decision policy that is equally applicable to any input provided to the process. Joshua Kroll and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633, 637–641.
[1026] Goodman and Flaxman (n 1008) 6; Selbst and Powles (n 1014) 235–237; Edwards and Veale (n 1007) 52.
[1027] Brkan (n 763) 112.
[1028] ibid 114; Edwards and Veale (n 1007) 52; Mendoza and Bygrave (n 793) 16.
[1029] Malgieri and Comandé (n 807) 254–255; Brkan (n 763) 115.
[1030] Mendoza and Bygrave (n 793) 17; Selbst and Powles (n 1014) 236; Brkan (n 763) 114.
[1031] Brkan (n 763) 116.

GDPR, in light of its high demands of transparency towards data subjects[1032], may also favour an extensive reading.

Despite the academic efforts to confer legal standing to a right to explanation, to date, there has been no clear acknowledgment for such a broad interpretation and the practice seems to prefer a cautious and narrower approach.

The comparative analysis of domestic legal systems confirms that most Member States did not complement or further specify GDPR information duties under national data protection laws[1033]. The only exceptions seem to be Hungary and France that make reference to a right to explanation/information in their national laws[1034]. However, from the contents of such rights, whose wording slightly differ between the two countries, it is not entirely clear whether an *ex post* explanation is envisaged[1035].

The guidance offered by the WP29 on the matter[1036] has also not provided conclusive evidence. Indeed, the WP29 opinion shows a preference for an enlightened interpretation of Art. 22 in view of Recital 71. However, when it comes to clarifying the contents of the notifications, the choice of terms is not always straightforward. The requirement that meaningful information about the system logic needs to be «sufficiently comprehensive for the data subject to understand the *reasons for the decision*»[1037] are followed by the indication that information on the envisaged consequences must be provided «about *intended or future processing*»[1038] and that, following an access request, the controller «should provide the data subject with information about the

[1032] See further also Antoni Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8 European Journal of Law and Technology; M Temme, 'Algorithms and Transparency in View of the New General Data Protection Regulation' (2017) 3 European Data Protection Law Review 473.

[1033] Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review 22. The comparative analysis covers nine EU countries (Italy, the Netherlands, Ireland, Germany, France, Hungary, Slovenia, Austria, Belgium) and the UK.

[1034] In Hungary the data controller should inform the subject about «the methods and criteria used in the decision- making mechanism». In France, the explanation should be based on the «rules defining the data processing and the main features of its implementation». ibid.

[1035] This is obvious for Hungary that does not make any distinction between information about the general functionality of the algorithm architecture and about practical implementation in a given case. On the contrary, according to Malgieri, France does in fact introduce also an *ex post* right to explanation that can be inferred from the requirement to provide the «main means of implementation», suggesting these may only relate to the practical implementation of the system. ibid. However, it could be argued that the term "implementation" is used in a rather general way to indicate the practical functioning of the system, not instead its functioning on an *ad-hoc* basis for each decision taken.

[1036] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478).

[1037] ibid 25.

[1038] ibid 26.

envisaged consequences of the processing, *rather than an explanation of a particular decision*»[1039].

Finally, cases concerning algorithmic transparency of automated decisions have started to surface also national courts[1040] and references to Art. 22 GDPR and controllers' information duties in the context of automated decision-making processes have made their first appearance in national rulings. The innovative tone of these decisions, however, does not provide meaningful insight with respect to the *type* of explanation that should be provided in practice, since references to the transparency of algorithmic decisions are still vague[1041].

3.2.2 Advantages of introducing/recognizing a right to explanation

Whether a right to explanation is already applicable or should instead be expressly introduced, as mentioned above, one of the main reasons advanced for its formal recognition revolve around the expected ability of the said right to fill the awareness gap that data subjects are currently experiencing when subject to automated-decision making process[1042]. By improving individuals' awareness, meaningful and personalized explanations would serve the effective exercise of the other subjective rights granted by the GDPR against automated-based decisions and, overall, would help individuals to regain some control over the processing of their data.

[1039] ibid 27.

[1040] See for example Italian Supreme Court of Cassation, decision n. 14381/2021; Italian Council of State, decisions n. 881/2020; n. 8472/2019 and n. 2270/2019 (dealing with algorithms and administrative procedures); Amsterdam District Court, case C/13/687315/HA RK 20-207 ("Uber case") and a C/13/689705/HA RK 20-258 ("Ola case"), 11 March 2021; Conseil Constitutionnel, decision n. 765/2018, 12 June 2018, https://www.conseil-constitutionnel.fr/decision/2018/ 2018765DC.htm (last access 17 August 2018).

[1041] In the Italian decision, the Court of Cassation refers to the «knowability of the algorithmic executive scheme» see Oreste Pollicino and Marco Bassini, 'La Cassazione Sul "Consenso Algoritmico". Ancora Un Tassello Nella Costruzione Di Uno Statuto Giuridico Composito' [2021] Giustizia Insieme <https://www.giustiziainsieme.it/it/news/127-main/diritto-e-innovazione/1800-la-cassazione-sul-consenso-algoritmico-ancora-un-tassello-nella-costruzione-di-uno-statuto-giuridico-composito> accessed 7 July 2021. In the Ola decision the Amsterdam District Court interprets "useful information about the underlying logic" in such a way that the most important assessment criteria and their role must be communicated to the data subject. See Raphaël Gellert, Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making' [2021] Eu Law Analysis blog <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html> accessed 7 July 2021.

[1042] Mendoza and Bygrave (n 793) 7; Selbst and Powles (n 1014) 237; Brkan (n 763) 111–112; Wachter, Mittelstadt and Russell (n 1012); Malgieri and Comandé (n 807).

3.2.3 Barriers to the effectiveness of a right to explanation

Whether promising in theory, the same proponents of a right to explanation do not hesitate to recognize that, even if formally recognized in practice, a number of legal and technical barriers would still jeopardize its effective and meaningful application for the purposes of enhancing individuals' control over data.

First, several scholars have warned against the limited number of situations that the right would cover, should it be linked primarily to Art. 22 GDPR, as it could apply only to those automated-decisions that meet the conditions listed in that article[1043]. As already mentioned, these conditions (e.g., being "based *solely* on automated processing" having "*legal effects*" and being grounded either on the performance of a contract or on the data subject's consent[1044]) would considerably narrow down the category of automated-decision making processes that could be subject to an explanation request[1045], thus essentially downsizing the incisiveness of this right.

Secondly, the right would still be affected by the technological and cognitive barriers already explored under Chapter II, par. 3.4. For an explanation to be meaningful, in fact, the latter should be (i) sufficiently exhaustive, but also (ii) comprehensible to the average user. However, as explored in detail in previous paragraphs, in the context of complex algorithmic decision-making processes, providing meaningful and transparent explanations is an increasing challenge[1046]. On the one hand, for many advanced systems, there is no theory correlating input variables and outputs (decision) through logical steps, understandable to humans[1047]. Advanced systems that work with thousands of variables and employ machine learning techniques to achieve their outcomes do not follow pre-determined logical paths, which makes the understanding of the functioning of the system, as well as the rationale underlying its specific outcomes extremely arduous, if not impossible[1048]. On the other hand, the limited cognitive abilities of end-users greatly impair the chances of providing them with meaningful elements that they could actually comprehend and put to use. In this respect, it seems sufficient to recall the many contributions quoted in previous paragraphs, that

[1043] Wachter, Mittelstadt and Russell (n 1012) 869 and 873; Wachter, Mittelstadt and Floridi (n 773) 92.
[1044] See above, Chapter II par. 3.4. and 4.1.
[1045] Other scholars (e.g. Malgieri and Comandé (n 807) 254.), however, sustain that a correct interpretation of the said conditions would prevent Art. 22(1) GDPR from being too narrowly (thus ineffectively) construed.
[1046] Wachter, Mittelstadt and Russell (n 1012) 850–851.
[1047] Edwards and Veale (n 1007) 59.
[1048] Brkan (n 763) 117; Edwards and Veale (n 1007) 59.

convincingly highlight the trade-off between accuracy and understandability. In brief, «optimising an explanation for human interpretability necessarily means diluting predictive performance to capture only the main logics of a system»[1049], which in turn makes the explanation inevitably poorer of meaningful information, raising question about its practical value[1050]. To overcome this impasse and preserving the meaningfulness, hence effectiveness, of a broad right to explanation, some scholars have proposed the adoption of alternative explanation mechanisms, following a user-friendly and "legal design" approach to information presentation. Wachter and others, for example, suggest the provision of "counterfactual explanations" of algorithmic decisions[1051], constructed in the form of "*if (x) – then (y)*" statements that would bypass the substantial challenge of explaining the internal workings/rationale of complex systems with practical examples and could be tailored on the data subject's specific situation[1052]. On the same lines, Veale and others consider as particularly effective the "exploring with explanation" method[1053], based on which individuals could hypothetically explore the logics happening around input data, understanding from inferences the underlying functioning of the system[1054]. In practice, this approach could be supported by the developments of tools that let users "try out" the system, by providing different inputs and comparing the resulting outputs[1055]. Finally, Malgieri and Comandè suggest to introduce a "legibility test", according to which controllers would be required to answer a questionnaire covering elements of both the system's technical architecture ("logic", i.e., internal functionality) and contextual implementation ("significance" and "consequences", i.e., purpose, impact, human involvement)[1056]. The questionnaire's outcomes would be then made available to data subjects, and, in light of the easy-to-understand structure but also detailed information on the practical use-cases, they would be able to meet the "meaningfulness" threshold of the explanation, combining

[1049] Edwards and Veale (n 1007) 59.
[1050] See e.g., Solove (n 57); Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution* (Cham: Springer International Publishing 2018); Frederik Zuiderveen Borgeswius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security & Privacy 103, further in Chapter II par. 2.2.
[1051] Wachter, Mittelstadt and Russell (n 1012).
[1052] ibid 843 and more extensively 860 ff.
[1053] Edwards and Veale (n 1007) 60–61.
[1054] ibid 62.
[1055] ibid 63. The authors, however, recognize how effective querying systems would be difficult to implement, since they would require users to provide credible inputs about hypothetical situations different from their own but «simulating the inputs of others convincingly is hard».
[1056] Malgieri and Comandé (n 807) 259–261.

both information transparency and comprehensibility. For all these proposals, it is not disputed the value they may have for technology experts, auditors and developers, to help them navigate the functioning of algorithmic systems and anticipate or correct potential errors and biases of the algorithm. However, it remains to be seen how much they would actually improve users' engagement and awareness. It is in fact still difficult to imagine how these explanations may achieve a satisfactory comprehension threshold and overcome the attention span and time constraints that individuals face in their daily lives.

In sum, the recognition (or introduction) of a broad right to explanation on automated-decision making processes may indeed help to foster algorithmic transparency, vesting controllers with the responsibility to provide more detailed and contextualized elements clarifying the underlying decision-making process employed. Taking into account both the limited scope of application and persisting cognitive and technological barriers, however, a few considerable obstacles persist to the effectiveness of this "new" right to properly enhance individuals' control over data processing.

3.3 Extending the scope of existing data subjects rights: the case of machine-learning models

Due to the complexity of the modern technological landscape, there are increasing situations that, despite being strictly connected with the use of personal data, elude and escape individuals' reach, leaving them essentially with no usable instruments to exert any form of control. "Machine learning models" are an example of this sort.

As briefly mentioned in the previous chapter, machine learning (ML) algorithms are revolutionizing the way in which data is analysed, exponentially improving their abilities to identify patterns, infer information and make accurate predictions[1057]. In the context of machine learning, systems turn training data into a "model" that can infer information, make predictions or classifications of new data on the basis of patterns distilled from the initial training set[1058]. Essentially, machine learning models represent the "way" or "logic involved"[1059] that the system learns and reproduce to achieve a certain output (prediction, classification), based on given input.

[1057] Sartor (n 162) 7 ff.
[1058] MR Leiser and Francien Dechesne, 'Governing Machine-Learning Models: Challenging the Personal Data Presumption' (2020) 10 International Data Privacy Law 187, 189.
[1059] The "logic" of the ML model refers simply to the dependency of the output on the input for a given task, namely it codifies correlations (according to a chosen metric and parameters that turn out to be

Much of the data that forms ML training sets is personal data. Further, ML models are fed with personal input relating to specific subjects, to infer information, make predictions and take decisions about them. However, since ML models themselves only represent the underlying (often obscure) reasoning followed by the system to achieve its output, individuals have no power to monitor and get insights around the construction of these models and investigate what they may tell about them, if used. While data protection rights are applicable *before* the model is built (i.e., on the personal data used to train the model), or *after* it is applied to a subject (i.e., on the decision resulting from the automated-decision making processes), there is a gap of control in the moment in which the model is developed and finalized[1060]. This leaves data subjects with no effective means to investigate on the model creation and obtain information over the finalized model, to understand how the latter may potentially "read" them, if used, (e.g., profile them, infer information, predict their behaviour), based on the data it was trained on[1061].

3.3.1 Machine-learning models as personal data

As a possible avenue to bring back into the control sphere of individuals these "loose" situations and provide individuals with some agency over ML models, some authors have proposed to extend the scope of existing subjective rights, by *de facto* expanding the scope of data protection law. Vaele and others, in particular, have advanced a suggestive proposal which elaborates on the idea that, under certain circumstances, ML models should be considered personal data, thus be subject to all the individual rights provided by the GDPR[1062].

The proposal of these authors appears to have drawn inspiration from a recognized trend, both at regulatory[1063] and jurisprudential[1064] level, towards a widened interpretation of the concept of "personal data". The definition of personal data adopted

effective and produce an accept- able margin of error), rather than causal dependencies or "logic" as we are used to think of. ibid 191.

[1060] Michael Veale, Reuben Binns and Lilian Edwards, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180083, 4.

[1061] ibid 3.

[1062] ibid 4 ff.

[1063] The WP29 opinion on the concept of "personal data" has endorsed a broad interpretation of the notion. Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (20 June 2007) WP 136.

[1064] The CJEU has also adopted a number of decisions that favoured an extensive interpretation of personal data. See for an overview, Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 59 ff.

under EU law is already very flexible and comprehensive, as it links the quality of "personal" to a series of attributes (e.g., *any* information; *related to*; *identified* or *identifiable*) that allow for a very broad interpretation[1065]. The advent of technological progresses, that are increasingly challenging the boundaries between anonymity and re-identifiability, have contributed to push the threshold of the "personality" character of information even further. In the age of the Internet of Things, advanced data analytics and data-driven decision-making, any information can eventually connect to and in some way identify a person in the meaning of EU data protection law[1066]. Expanding the scope of the notion enabled therefore to catch evolving forms of data processing emerging from technological developments within the reach of protection of data protection law. The reactions to this expansive tendency have been different. Some have been very critical of a concept of personal data growing too broad, as it would render the data protection regime simply unmanageable thus ineffective[1067]. Others, despite recognizing the possible long-term disruptive impacts, welcomed an extensive definition of personal data and the consequent broad scope of protection on the basis that «if all data has a potential to impact people and is therefore personal, all data should trigger some sort of protection against possible negative impacts»[1068].

Vaele and others do not specifically endorse this broadening trend, and, on the contrary, argue that their claim of ML models falling under the definition of personal data «does not depend on the kind of expansive definition that gives rise to» the risks of data protection maximalist mentioned above[1069]. However, they indeed challenge the traditional understanding of the definition of personal data and rely on a very peculiar interpretation of this definition.

The argument advanced by these authors develops in the following way. Evidence has shown that models exposed to certain confidentiality attacks (more precisely "model

[1065] Recalling here the definition of "personal data" provided by the GDPR that reads «means *any information relating to* an *identified or identifiable* natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person».
[1066] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 1064) 42.
[1067] See e.g., Ohm (n 687).
[1068] Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (n 1064) 42 and 72.
[1069] Veale, Binns and Edwards (n 1060) 8.

inversion"[1070] and "membership interference"[1071] attacks) may "leak" personal data that they were trained with. According to the authors, ML models may thus be compared to "pseudonymized" versions of their training personal data, that when exposed to a particular "key" (i.e., a confidentiality attack) can reveal the re-identified data underneath[1072]. Hence, they conclude, that when models are vulnerable to such attacks, they should also be considered *per se* personal data[1073]. The main consequence for data subjects would be the possibility to exercise their subjective rights against the model itself. In particular, they would be able to (i) receive information on the origin of the model, therefore know whether the model was trained by a third party and subsequently sold; (ii) request to be erased from the model (e.g., to erase insights they may dislike) and (iii) object to the use of the model[1074].

3.3.2 Criticisms to the ML model as personal data proposal

The provocative proposal described above was subject to various critiques. Leiser and Dechesne, in particular, criticize the claim made by Veale and others on the basis that it was developed on a misunderstood conception of how ML models actually work[1075] and how re-identification may eventually occur[1076]. Even admitting, for the sake of discussion, that models could be classified as personal data, a number of questions still remain especially on the effectiveness of such solution. First, the limited scope of the proposal: adopting this approach, models that are not amenable to inversion attacks would fall outside the scope of protection. However, they may still be predictive and profiling models that individuals wish to know the origin or destination of, or wish to have themselves or their group erased from[1077]. Secondly, echoing the general concerns over an extended definition of personal data, the scale of the GDPR resulting from its

[1070] "Model inversion attacks" are aimed at reconstructing training data from model parameters. A data controller, who does not initially have direct access to the (A) trained data, but is given access to (B) the trained model and (C) a different set of variables that include data relating to persons' include in the training data set, is able to recover some of the variables in (A), using (C), due to their connection with (B). ibid 5.
[1071] "Membership inference attacks" do not recover training data, but instead ascertain whether a given individual's data were in a training set or not. Leiser and Dechesne (n 1058) 194.
[1072] Veale, Binns and Edwards (n 1060) 6.
[1073] ibid 7.
[1074] ibid 8–10.
[1075] The model itself does not contain personal data per se, nor reveal it. It requires purposeful action of a nefarious actor seeking to reveal the personal data, for example, the re- construction of the black box model into a shadow model for the purpose of revealing information from the training data. This should count as improper use of the model. We do not have to look for a solution in terms of strict data protection if we already have a body of work regulating bad behaviour. Leiser and Dechesne (n 1058) 191.
[1076] The actual reidentification is not done by the model but by a skilled human. The data in itself only become personal data on the basis of external inferences. ibid 192.
[1077] Veale, Binns and Edwards (n 1060) 12.

widened scope of protection makes its rights and obligations unmanageable for individuals[1078]. Thus, increasing the material scope of data protection rights does not appear to be an efficient solution to restore individual control over personal data, when the ultimate burden to exercise these rights needs to be borne by the data subjects themselves.

4 Conclusions

The investigation conducted in this Third Chapter has offered an overview of proposed solutions that have been advanced, and in some cases are already in the process of being implemented, to fill existing control gaps and support individuals in the exercise of a more aware and effective control over the processing of their personal data.

Below, a table summarizes the findings analysed in this section, their envisaged effects and the persisting issues they are not able to solve or that may limit their effectiveness.

Response	Effects	Issues
PETs	- More effective control and management of privacy preferences - Easier exercise of GDPR rights	- Poor market penetration and consumers' engagement - Lack of standardization and weak technical feasibility for a centralized and comprehensive management tool - Difficult allocation of privacy roles - Arguable improvement in data subjects' awareness
Positive nudges	- Guide individuals towards "better" privacy decisions - Mitigate certain inherent biases	- Implementation uncertainties - Obsolescence-related issues - Doubts on their effectiveness in improving individuals' behaviours
Right to property	- Strongest form of "individual control" - *Erga omens* protection - More transparent and efficient data transfer system	- Difficulties to micro-manage day-by-day data processing situations due to the scale of data processing - Persisting information asymmetries and bounded rationality issues - Limited scope (private sector)

[1078] Leiser and Dechesne (n 1058) 199.

		(+ issues on a possible "commodification" of the individual, costly implementation of the system, conflicts with other interests)
Right to explanation	- Increases the degree of awareness and enhances the possibility for data subjects to influence automated decision - Better exercise of the other safeguards in the context of solely automated data processing	- Limited scope of the right (many algorithmic decision-making processes may fall outside the scope of the provision) - Difficult to exercise due to conflicts with controllers' IP rights - Persisting cognitive challenges of providing a "meaningful" and "comprehensible" explanation (+ no common agreement on the existence of such right)
Extending the scope of data subject's rights ("ML model" as personal data)	- Extends the range of control individuals can exercise against algorithmic models (before they are applied in practice)	- Limited scope of protection (only models vulnerable to inversion and inference attacks) - Worrying trend to expand the definition of personal data, making the overall data protection system unmanageable

Table 11. Mechanisms to support individual control

Technically-oriented solutions appear to have greater potential than those proposed in the legal domain, both in terms of practical application and envisaged effectiveness.

Technical solutions, like PETs, try to tackle the complexity and ubiquity of the current data ecosystem, providing data subjects with the technological means to enable them to track and influence the circulation of their data. Nudging interventions, whether in the soft form of "legal design" approaches or in the more intense one of defaults and incentives, are instead primarily focused on data subjects' cognitive limitations, which they try to mitigate by improving the background against which individuals make their privacy decisions.

Leaving aside the thorny debate over the propertization of personal data, which in any case as concluded above is not expected to add much to the individual control cause, the introduction of new subjective rights intends to enrich the catalogues of legal means that users could exercise vis-à-vis controllers, with instruments better tailored to the novel needs stemming from the evolving machine-driven context.

While each of the proposed solutions faces pending challenges that may obstacle their prompt adoption, they set promising ground to improve, albeit within their own scope, the condition of data subjects.

At the same time, the analysed mechanisms show that providing data subjects with additional tools or more rights in many cases is not enough to secure them from the dangers of processing activities. Certain weaknesses of the individual control paradigm are particularly difficult to eradicate, considering they originate from the combination of intrinsic human biases and the intricacies of a technological context that shows no sign of slowdown.

Even when provided with innovative instruments, the complexity of the modern data processing environment can easily overwhelm users, who may still not have proper oversight and understanding on how their data are used and what the consequences of such uses may be, particularly when these entail externalities involving groups and collectivity. They may still lack the time and economic resources to take personally care of their day-by-day data management. They may still be obstructed in the exercise of their rights, manipulated or deceived without having any knowledge of it.

In light of these considerations, that prove how relying on individual-centric mechanisms does not provide sufficient guarantees of success, the next chapter will consider whether other mechanisms outside the data subject limited sphere of action should be better leveraged to both support individuals in their control mission, but also complement their inevitable loopholes when they fail to protect themselves.

CHAPTER IV – Complementing the individual control model

1 Introduction

The conclusions in Chapter Three indicate that providing data subjects with additional instruments to exert their control rights is not alone sufficient to overcome some inherent limitations of the individual control model. Given the complexity and ubiquity of data processing situations, individuals, in many cases, still lack sufficient oversight capacities, comprehension abilities and enforcement powers to make their control effective.

This Fourth Chapter explores mechanisms and proposals that move beyond a strict "data subject-focused" dimension. Characteristic of these mechanisms, in fact, is that they: (i) are addressed primarily to different societal actors rather than data subjects, therefore do not rely (or not primarily) on the capacities of individuals; and/or (ii) can address data protection issues from a broader collective and social dimension, rather than considering it a matter of individual choice and preferences.

These mechanisms are not intended to fully replace individual control, rather they help to create a broader "control" structure that both helps to ensure that individuals are put in the proper conditions to exercise their rights effectively and consciously (thus they directly support the individual control model itself), but also supplement the protection gaps left by the individual control approach, when it is inherently not apt to assess and stand against the threats that data processing activities may pose to individuals, groups and society at large.

The different solutions explored hereinafter group, indifferently, measures that are already included in the GDPR framework but have not yet been adequately strengthened, encouraged or explored to become successful supplementary mechanisms; measures that have been proposed and are under development, but have not gained sufficient popularity, nor formal legal recognition; and measures that are emerging in the context of other policy initiatives that may improve, although are not primarily addressed to, the protection of personal data.

2 Improving the "architecture of empowerment"

Data protection legislation has not been completely blind towards the inability of individuals to act alone to protect their privacy interests.

The DPD, first, and more evidently the GDPR have placed individuals and their rights in a broader infrastructure that involves other societal actors. They together form what has been defined an "architecture of empowerment"[1079]. The architecture builds around the engagement of a variety of subjects, beside individual citizens, in the governance of data flows and processing: supervisory authorities, NGOs, media, activists, academics. Regardless of whether their functions are expressly recognized by law, such as for DPAs (Articles 51-59 GDPR) and representative entities (Art. 80 GDPR), or not, like in the case of the media and academia, they all are essential pieces to develop a robust "ecology of transparency"[1080], namely a network of intra-institutional relationship between regulators, civil society actors, norms and practices[1081], whose combined efforts make it possible to penetrate the shadows of the digital ecosystem, and scrutinize it.

This network of stakeholders, in fact, appears to have the powers, resources and expertise to substantially compensate for some of the weaknesses posed by the individual control model. First, they are better placed to monitor that controllers enable individuals to be in the right conditions to effectively exercise their control rights (e.g., in terms of effective consent and exercise of their GDPR rights), in this way ensuring that when "control" is claimed it is not illusory. Secondly, they are in a better position to assess the dangers and harms of processing activities, mitigating cognitive limitations and biases of single individuals. Thirdly, they have stronger means and authority to make sure controllers process personal data in a fair and lawful manner.

2.1 Boosting the role of Data Protection Authorities

Possibly the most developed and consolidated pillar of the broader architecture of empowerment are data protection authorities (DPAs). Their institution is a typical feature of EU data protection law[1082]. Conceived since the early phases of data

[1079] René Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' (LawArXiv 2020) preprint 10.
[1080] "Ecology of transparency" is a term originally employed by Kreimer in the context of the Freedom Of Information Act (FOIA), that provides citizens with rights to know about the functioning and decision making of governmental bodies, to highlight the existence of a broader network of «tenacious requesters», well-financed NGOs and active media that complemented and supplemented those rights, to achieve transparency in practice. Seth Kreimer, 'The Freedom of Information Act and the Ecology of Transparency' (2008) 10 University of Pennsylvania Journal of Constitutional Law 1011. Mahieu et al. transposes the term in the data protection context. Mahieu, Asghari and van Eeten (n 789).
[1081] Mahieu, Asghari and van Eeten (n 789) 4.
[1082] Peter Hustinx, 'The Role of Data Protection Authorities' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 131–132.

processing regulations in Europe, their role as fundamental watchdogs of data protection compliance has been steadily consolidating over the last fifty years.

Back in the '70s, the first national acts governing data practices already included some form of supervision by external bodies, endowed with certain monitoring tasks and enforcement powers to ensure compliance with the rules on processing activities[1083]. From there on, the provision of local public bodies (differently named "commission", "commissioner", "authority", "registrar", "inspectorate", "guarantor") with oversight and corrective powers has been a recurring aspect of all the subsequent national data protection laws[1084]. Despite an unsatisfactory attempt of harmonization at EU level under the DPD[1085], proper consolidation of these authorities was achieved only with the GDPR. The mission of supervisory authorities and their essential role in the data protection framework has been ultimately crystallized under Art. 8(3) of the EU Charter[1086], which makes them the only authorities explicitly mentioned in primary law[1087]. As Hijmans notes, due to the said inclusion under primary law, DPAs are «a unique phenomenon in EU law»[1088], since «control by these authorities is not only an essential part of enforcement, it is even qualified as an "essential component of the protection" itself»[1089].

This strong regulatory anchorage, as well as the specific role, characteristics and powers assigned by law are what makes DPAs best suited to compensate for the weaknesses and fallacies of individuals in the protection of individual rights and collective interests.

2.1.1 Role of DPAs

The role of "data protection enforcer" has been an identifying trait of DPAs since their early institution. The 1970 Hessen Data Protection Act charged its "Commissioner" with the duty «to ensure compliance with the provision of the act»[1090], the 1978 *Loi Informatique* assigned the "National Commission" the task to monitor that automated

[1083] See Chapter I, par. 5.2.
[1084] See Chapter I, par. 5.2 and Bygrave (n 14) 70–71.
[1085] See above Chapter I, par. 5.1.
[1086] Supervisory authorities are also mentioned under Art. 16 TFEU, that confers powers on the European Union to act in the domain of privacy and data protection. See Licia Califano, 'Il Ruolo Di Vigilanza Del Garante per La Protezione Dei Dati Personali' (2020) 33 federalismi.it 2.
[1087] Art. 8(3) of the EU Charter states: «Compliance with these rules [*set forth under par. 2*] shall be subject to control by an independent authority».
[1088] Hijmans, *The European Union as Guardian of Internet Privacy* (n 416) 564.
[1089] ibid.
[1090] Art. 10(1) Hessen Data Protection Act.

processing were «carried out in compliance with the provisions of the law»[1091] and the 1995 DPD envisaged for supervisory authorities the responsibility to monitor «the application within its territory of the provisions adopted by the Member States pursuant to this Directive»[1092]. Now, the GDPR invests DPAs with the duty to monitor «the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union»[1093].

2.1.2 Independence and expertise

Independence and expertise are two essential characteristics that consolidate the role of DPAs as primary guardians of data protection. “Complete independence” from direct or indirect influences[1094] provides these authorities the necessary autonomy and instruments to effectively perform their functions from external pressures, whether by market players and other private actors or political powers[1095]. As repeatedly stated by the CJEU[1096] and other EU institutions[1097] , however, independence is possible only when proper human, technical and financial resources, are granted.

Further, DPAs are “expert bodies”[1098]. The possession of comprehensive knowledge and adequate expertise in data protection is a necessary pre-condition to determine the lawfulness and correctness of processing activities. This does not only entail in-depth understanding of the normative aspects of the sector, but also considerable familiarity

[1091] Art. 14, *Loi Informatique*.
[1092] Art. 28(1) DPD.
[1093] Art. 51(1) GDPR.
[1094] Art. 8(3) EU Charter and Art. 52 GDPR. The principle has been stated and clarified on several occasions by the CJEU case law. For an overview of the main decisions, see Paul De Hert, ‘Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism’ in Stefano Montaldo, Francesco Costamagna and Alberto Miglio (eds), *EU Law Enforcement The Evolution of Sanctioning Powers* (Routledge 2021) 301.; Francesco Cardarelli, ‘Indipendenza e autorità di controllo’ in Roberto D’Orazio and others (eds), *Codice della privacy e data protection* (Giuffrè Francis Lefebvre 2021) 708–711.
[1095] De Hert (n 1094) 301. Elena Guardigli, ‘Le Autorità Di Controllo: Dalla Direttiva 95/46/CE al Regolamento n. 679/2016’ in Giusella Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101* (Prima edizione, Zanichelli editore 2019) 679–670.
[1096] The subject-matter was dealt in particular in Case C- 614/10, *Commission v of Austria* [2012] ECLI:EU:C:2012:631, see Cardarelli (n 1094) 718–719.
[1097] See e.g. Article 29 Data Protection Working Party, ‘Opinion 1/2012 on the Data Protection Reform Proposal’ (23 March 2012) WP 191 8. European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - “A Comprehensive Approach on Personal Data Protection in the European Union”’ (14 January 2011) 28; European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the Data Protection Reform Package’ (7 March 2012) 38.
[1098] Hijmans, *The European Union as Guardian of Internet Privacy* (n 416) 347–412.

with its characteristic technological developments[1099], given the increasing complexity and technicality of processing activities. While average users lack the skills to achieve this level of expertise[1100], supervisory authorities should in principle have the necessary competences and resources to be well-equipped before any legal or technological development in the field. Even at their infancy, the specialized nature of these bodies was recognized as one of their main qualities[1101]. Simitis, for example, underlined how these authorities «have the necessary knowledge enabling them to analyse the structure of public and private agencies and to trace step by step their information procedures. They can therefore detect deficiencies and propose adequate remedies»[1102]. Particularly under the GDPR, this expertise component has been further emphasized. Art. 53(2) GDPR expressly provides that each DPA's member needs to «have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers», setting a preliminary quality threshold to access the authority. No further details have been provided on the "type" of skills required. However, the importance of keeping abreast of market technological progresses can be inferred from the inclusion among the DPA's duties of the task to monitor relevant developments, when they have an impact on the protection of personal data, in particular «the development of information and communication technologies and commercial practices»[1103].

2.1.3 Tasks and powers

As glimpsed in Chapter I, the early data protection period ('70s-'80s) was characterized by very interventionists DPAs, endowed with strong preventive powers of review and authorization. The adoption of extended licensing/authorization schemes, notification and registration procedures allowed DPAs to assess and approve (or block) processing operations before they were put into practice[1104].

[1099] Hustinx, 'The Right to Informational Self-Determination and the Value of Self-Development' (n 1082) 132–133.
[1100] As extensively highlighted in Chapter II.
[1101] Flaherty, for example, describing supervisory authorities, positively stressed the fact that «each agency has specialists in various types of information systems and data flows who can speak intelligently about data protection and security with the operators of government information systems». Flaherty, *Protecting Privacy in Surveillance Societies* (n 3) 383.
[1102] Council of Europe (n 66) 177.
[1103] Art. 57(1)(i) GDPR.
[1104] See Chapter I, para. 2-4 on the evolution of the *ex-ante* control mechanisms provided in the early-generations laws.

In subsequent laws, up to the DPD, this *ex-ante* review approach, unable to cope with the mounting volume of data processing, was progressively reduced in favour of a less burdensome *ex-post* monitoring model, that focused on stronger monitoring and enforcement functions towards ongoing processing activities and limited prior-authorization powers to a few provisions[1105]. Accordingly, the tasks of DPAs started to be more nuanced and diversified. Traditional oversight and enforcement tasks were complemented with awareness activities for the promotion of "privacy culture"[1106]. Investigatory powers became more articulated[1107]. Enforcement and intervention capacities were expanded, including actions that ranged from mild warnings to more penetrating destruction orders or bans on processing[1108] and, depending on the regulatory choices of member states, DPAs could also be endowed with the power to impose administrative fines[1109]. Despite the attempts to encourage transnational cooperation[1110], cross-border initiatives between national DPAs were not "institutionalized" through clear rules and time frames, and took place mostly on an informal basis[1111]. When successful, transnational cooperation was mainly the result of spontaneous collaborations[1112].

However, national legal fragmentations over tasks and powers of DPAs, poor trans-national cooperation, and the obsolescent framework of the DPD[1113] according to which

[1105] See Chapter I, para. 2-4 and further 5 on the DPD for a comparison on the enhanced role of *ex post* rather than *ex ante* mechanisms.
[1106] Despite it is not mentioned under the DPD, this task was expressly included in the privacy law implementing the DPD (Art. 31(1)(i), l. 675/1996), and restated in the subsequent Italian Privacy Code (Art. 154(1)(h), dlg.s 196/2003). Califano (n 1086) 9.
[1107] The DPD included specifications on «powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties».
[1108] Art. 28(3) DPD, provided a range of different corrective measures that had to be implemented at national level.
[1109] The DPD did not directly assigned to supervisory authority the power to issue sanctions and left member state free to determine which authority/body could apply sanctions, based on national law, as well as the type of sanctions (administrative/criminal/civil) available. As a consequence, states adopted different sanction regimes, some more focused on administrative sanctions and supervisory bodies, others more on criminal sanctions and judicial proceedings. Andra Giurgiu and Tine Larsen, 'Roles and Powers of National Data Protection Authorities' (2016) 2 European Data Protection Law Review 344 <https://orbilu.uni.lu/handle/10993/29819> accessed 29 October 2021; Bygrave (n 14) 172.
[1110] The DPD included very high-level duties of cooperation between DPAs, in particular on the exchange of useful information. With a view to coordinate a "structured network of DPAs" it created the Article 29 Working Party, formed by representative of national DPAs. Hijmans, *The European Union as Guardian of Internet Privacy* (n 416) 373.
[1111] Giurgiu and Larsen (n 1109) 346.
[1112] Califano (n 1086) 13.
[1113] The challenge to apply the DPD in a modern age of processing activities was confirmed by the case-law of the CJEU that, before the GDPR, more than once "stretched" the powers and competences of

they had to act undermined the impact supervisory authorities could have on effective enforcement.

The GDPR has tried to overcome these shortcomings. With a view to reinforce the role of DPAs as "guardians of data protection" [1114], the GDPR upgrades the previous framework following three main lines of action.

(i) Enhanced monitoring and corrective powers – The GDPR includes a clear list of tasks and powers equally applicable to all EU DPAs. Renewed emphasis is placed on the monitor and enforcement duties assigned to DPAs to ensure compliance with the regulation, which include the task of "conducting independent investigations" on the application of the regulation but also "handle complaints", lodge by data subjects and "investigate their subject matter" [1115].

The increased emphasis on the "privacy watchdog" function of DPAs is confirmed by the amplified and detailed list of "investigatory powers" and "corrective powers" mentioned under Art. 58 GDPR[1116]. The formers endow the authorities with a range of instrument (e.g., audits; document access requests; access to premises) that intensify the possibility for authorities to scrutinize and shed light on the activities controllers carry out "behind the curtains". The latter, instead, include a set of corrective instruments, such as warnings and compliance requests; bans on processing activities and administrative sanctions, particularly severe under the GDPR[1117], that DPAs can issue to prompt compliance with data protection rules and punish their violations.

(ii) Prior authorization and awareness – Consistently with the path of gradual abandonment of prior control mechanisms in favour of a *ex post* monitoring and enforcement, the GDPR reserves little room for prior notification/authorization[1118]. A resemblance is maintained only in the mandatory prior-consultations that DPAs need to provide controllers, upon their request, when processing operations that are

DPAs to ensure an effective enforcement of the right to data protection. Giurgiu and Larsen (n 1109) 345–347.

[1114] As defined by the CJEU in case C-518/07 *Commission v Germany* [2010], ECLI:EU:C:2010:125.

[1115] Art. 57(1) GDPR. Cardarelli (n 1094) 744.

[1116] Art. 58(1) and (2) GDPR. These include the power to carry out investigations and require the cooperation of controllers and processors in the performance of audits, provision of information and access to their premises; the power to issue warnings and reprimands, to impose compliance measures and administrative fines to violators. See further Guardigli (n 1095) 676–681.

[1117] Art. 83 GDPR. Depending from the violation, these can go as high as 20 millions or for undertaking up to 4 % of the total worldwide annual turnover of the preceding financial year.

[1118] Califano (n 1086) 12.

covered by Art. 36 GDPR are involved[1119]. In addition, DPAs formally take up a primary role in fostering "public awareness" in data protection topics and issues, which reinforces the educational role that these entities held for the community.

(iii) Structured cooperation – Among the true highlights of the reform, alongside the exacerbation of pecuniary fines, is the creation of a European supervisory network, far more structured and dynamic than the inadequate cooperation provisions set forth in the previous framework. The GDPR puts an end to the "administrative isolation"[1120] of national authorities, and creates an EU governance that acts on two levels.

Horizontally, the GDPR intensifies the cooperation mechanisms between national DPAs, in three directions. It introduces the "one-stop-shop" mechanism[1121], whereby controllers doing business in more EU states can refer to a single DPA located in their own country ("leading authority")[1122], that will then involve and consult with the other interested DPAs when decisions/provisions against the company need to be taken; a system of "mutual assistance", through which DPAs exchange documents and information[1123]; and the possibility to conduct where appropriate "joint operations", including joint investigations and enforcement[1124]. Vertically, the GDPR establishes the European Data Protection Board (EDPB), that replaces the old representative body of DPAs at EU level, the WP29, and among its different functions[1125] plays a fundamental role in the context of the so called "consistency

[1119] It is the case for example of the "prior checking" (Art. 20 DPD) or subsequently "prior consultation" (Art. 36 GDPR) procedures, where data controllers are required to consult and obtain green light from the DPA before initiating data processing that may entail a particular risk for data subjects. More extensively used under the DPD, as transposed into national laws, this procedure has become very marginal under the GDPR as it has been relegated only to cases that, after conducting an impact assessment, continue to present a «*high risk in the absence of measures taken by the controller to mitigate the risk*».
[1120] Califano (n 1086) 13.
[1121] Art. 60 GDPR, see further Francesco Cardarelli, 'Cooperazione, assistenza e operazioni' in Roberto D'Orazio and others (eds), *Codice della privacy e data protection* (Giuffrè Francis Lefebvre 2021) 757 ss. Opponents of this mechanism argued it contrasted with the jurisdiction territorial principle of "proximity", according to which individuals were entitled protection by the DPA in the member state where they resided. Also, many opponents did not trust in the effectiveness of DPAs in other countries. De Hert (n 1094) 306.
[1122] Article 29 Data Protection Working Party, 'Guidelines on the Lead Supervisory Authority' (13 December 2016) wp244rev.01.
[1123] Art. 61 GDPR.
[1124] Art. 62 GDPR.
[1125] Art. 70 GDPR enumerates a number of tasks that the EDPB exercises in complete autonomy, such as advising the EU Commission, issuing guidelines and recommendations and review their application, promote awareness initiatives.

mechanism"[1126]. Under this mechanism, the EDPB performs coordination and dispute resolution functions, when investigations and decisions need to be taken by multiple DPAs, especially in the context of the one-stop-shop mechanism[1127].

The short overview above shows how independent supervisory authorities are entities structurally and functionally designed to carry out an effective control on processing activities and take action to protect data subjects, both to support the individual control model and compensate for some its weaknesses.

Supervisory authorities have the instruments to carry out an in-depth and intense scrutiny on processing activities of data controllers. They have (at least on paper) the expertise and resources to better overview and assess individual and collective risks posed by processing activities, compared to the limited cognitive abilities of individuals; at the same time, they monitor on the effective exercise of data subjects' rights. Further, they have the means and powers to block and sanctions behaviours in violation of data protection. "Hard enforcement" through the imposition of strong sanctions remains surely one of the most powerful instruments in the DPA toolbox[1128], further strengthened by the cooperation mechanisms introduced by the reform.

2.1.4 Current issues undermining the role of DPAs

Three years after its application, the GDPR has undoubltly brought visible improvements in the effectiveness of DPAs' activities to raise the level of data protection compliance and tackle the dangers posed by modern processing activities. Authorities have enhanced their monitoring activities on sensitive thematic areas (children's privacy, international data transfers, ads/marketing practices), increasing audits and inspections and actively engaging in a number of awareness initiatives[1129]. Also, in

[1126] See Felix Bieker, 'Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice' in Anja Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps*, vol 498 (Springer International Publishing 2016) 135. According to Hielke, «whereas the Commission saw a level playing field as an important rationale of the consistency mechanism, the outcome is mainly a conflict solving mechanism, to avoid problems where the views of the DPAs in a specific case diverge». Hence, the mechanism potential to impose consistency is reduced, but remains a valid instrument to incentivize uniform enforcement. Hielke Hijmans, 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?' (2016) 2 European Data Protection Law Review 362.

[1127] Art. 65 GDPR, see Bieker (n 1126) 135. Hijmans, 'The DPAs and Their Cooperation' (n 1126) 370.

[1128] Hielke Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?' (2018) 4 European Data Protection Law Review 80, 3.

[1129] Sebastião Barros Vale, Gabriela Zanfir-Fortuna and Rob Van Eijk, 'Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022' (Future of Privacy Forum 2021).

terms of "hard enforcement", the numbers in this area show a positive trend, with steady increase in the amount and quantity of fines issued[1130].

Beyond these signs of improvement, several issues still stand unaddressed, causing the effectiveness of DPAs' action to be increasingly subject to intense scrutiny. Inaction, low responsiveness rates and slow enforcement have led many voices to manifest how the new flagship legislation hasn't been able to "show its teeth yet"[1131] and is turning into frustration the initial hopes and expectations[1132].

(i) HARD ENFORCEMENT – A first set of issues concerns the "hard enforcement" aspects. A considerable number of complaints remains in fact unaddressed[1133]. This, in turn, slows down complaint-led investigations, reduces the chances of prompt enforcement and ultimately weakens the credibility of the system. At the same time, an inefficient management of incoming complaints will inevitably focus DPAs' energies in reducing the growing backlog, leaving less room for autonomous investigations in critical sectors, which are crucial to identify the often more obscure and dangerous processing practices, that may elude individuals' awareness. While slow complaint resolution, delays in proceedings and absence of fines affect most DPAs, these issues become even more critical when the concerned DPA plays a particularly strategic role in the enforcement arena. This is the case of the Luxembourg DPA or the Irish DC which are often "lead authorities" in a significant number of high-profile cases involving big tech companies (Google, Facebook, Twitter, WhatsApp, or Microsoft), that have set their main establishment in those countries[1134]. This inertia does not only result in major gaps in the protection of individuals around the EU, but it also undermines the general deterrence effect that a more expeditious and decisive action may produce. In addition,

[1130] For example, from May 2018 to October 2021, DPAs levied a total of 827 fines. Of the latter, the first ten fines are above € 10 million and the top three above 50 (Google, € 50 million; WhatsApp, € 225 millions; Amazon Europe, € 746 millions. Statistics taken from https://www.enforcementtracker.com/?insights, lastly accessed on 30 October 2021. See also European Data Protection Board, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' (5 August 2021).

[1131] Adam Satariano, 'Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates - The New York Times' *The New York Times* (27 April 2020) <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html> accessed 1 November 2021.

[1132] Access Now, 'Three Years under the EU GDPR' (Access Now 2021) 2 <https://www.accessnow.org/gdpr-three-years/>.

[1133] ibid 9.

[1134] See the criticisms raised by the German DPA and the EU Parliament against the Irish DC, Derek Scally, 'Irish Data Regulator Sparks Row with EU Colleagues on Facebook Oversight' (*The Irish Times*) <https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065> accessed 1 November 2021.

the analysis of fines reveals an inconsistent enforcement of EU law across Europe, that does not only highlight the persistence of different approaches in DPAs enforcement of data protection rules, but it also confirms a prominent difference between very active DPAs and passive ones[1135].

(ii) RESOURCES AND EXPERTISE – Nearly all DPAs lack adequate financial, human and technical resources to perform their functions[1136]. Although after the adoption of the GDPR some have received additional funds, these remain highly insufficient to face the growing number of incoming complaints and the high-costs of complex investigations[1137]. Cuts in staff and budget directly impact also on the level of technical expertise available in the DPAs structures, which is already very variable from authority to authority[1138] and is likely to be increasingly questioned in light of the technical competences required to effectively monitor the evolving technological landscape[1139].

(iii) COOPERATION - Practical complexities render coordination efforts between DPAs still lengthy and cumbersome. DPAs have been increasingly vocal on the issues they face when seeking to apply the one-stop-shop mechanism. They attribute these difficulties to the inadequate communications tools currently used to coordinate efforts, share information and follow cases[1140]; to existing procedural differences at national level in the handling of complaints[1141]; and to the lengthy duration of the processes[1142].

[1135] Brian Daigle and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' [2020] Journal of International Commerce and Economics <https://www.usitc.gov/journals>.

[1136] Already back in 2010, the EU's Fundamental Rights Agency had identified in understaffing and lack of financial resources a cause for the ineffective exercise of DPAs' tasks. European Union Agency for Fundamental Rights, *Strengthening the Fundamental Rights Architecture in the EU.II, Data Protection in the European Union : The Role of National Data Protection Authorities.* (Publications Office 2010). The issue persists still nowadays, see Access Now (n 1132) 10–11.

[1137] Sam Clark, 'Exclusive: Strained Irish Data Regulator Gets Big Staff Boost' Global Data Review (7 May 2021) <https://globaldatareview.com/data-privacy/exclusive-strained-irish-data-regulator-gets-big-staff-boost> accessed 1 November 2021.

[1138] Brave, 'New Data on GDPR Enforcement Agencies Reveal Why the GDPR Is Failing' (Brave 2020) <https://brave.com/dpa-report-2020/> accessed 1 November 2021.

[1139] Charles Raab and Ivan Szekely, 'Data Protection Authorities and Information Technology' (2017) 33 Computer Law & Security Review 421.

[1140] Access Now (n 1132) 13 ss.

[1141] European Data Protection Board, 'Individual Replies from the Data Protection Supervisory Authorities' (2020) <https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en> as quoted in ; Access Now (n 1132) 15.

[1142] European Data Protection Board, 'Individual Replies from the Data Protection Supervisory Authorities' (n 1141) as quoted in ; Access Now (n 1132) 15.

2.1.5 Concluding remarks

Since the early days, DPAs have acted as the main guardians of data protection. The tasks and powers that the GDPR endow them with provide these authorities, at least on paper, with the instruments and resources to be best placed to protect individuals when they are not capable or able to protect themselves. DPAs supplement the short-sighted vision that data subjects often have on data processing activities; ensure their rights are respected, hence that their "control" is effective, but also more broadly that processing activities which pose dangers for individuals and the collectivity in general are stopped and sanctioned.

Yet, as shown above, the effectiveness of DPAs' action to fulfil this "guardian" role is not satisfactory and further efforts are still required. A first urgent point is for governments to increase the financial and human resources allocated to DPAs, which are necessary for them to function properly and efficiently[1143]. This would help to speed up complaint handling and investigations, increase authorities' technical competences and improve enforcement effectiveness. Additional resources alone are not sufficient to cope with the mounting request for enforcement. DPAs need to act strategically, exploring innovative individual complaint management mechanisms[1144] and encourage collective complaints by NGOs and other representative actors to bring to the attention of DPAs the most pressing issues, and prioritize their activities in strategic sectors. Above all, the joining of DPAs' forces and resources through the use of all the cooperation instruments available under the GDPR is what could make a real difference against the "disproportionate resources" of tech firms[1145], without GDPR enforcement being an uneven burden for few authorities[1146]. To achieve that, the EDPB should fully embrace

[1143] To achieve this objective, some suggest the EU Commission may launch infringement actions against states which do not provide sufficient resources. Access Now (n 1132) 20.
Although it is unlikely this strict line of action will ever be taken, a more outspoken and vigorous position of the Commission on this subject may help as a stimulus for governments to ensure adequate resources.
[1144] Hijmans for example, supporting a proposal advanced by Hodges, suggests to consider an alternative mechanisms based on an external "ombudsman-system" for complaint management. Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?' (n 1128) 5.
[1145] Ken Foxe, 'Data Protection Commission "Acutely Strained" by Big Tech Cases' (*The Irish Times*) <https://www.irishtimes.com/business/technology/data-protection-commission-acutely-strained-by-big-tech-cases-1.4457683> accessed 1 November 2021.
[1146] European Data Protection Supervisor - European Data Protection Board, 'GDPR: A Three-Year-Old Who Must Still Learn to Walk before It Runs | European Data Protection Supervisor' <https://edps.europa.eu/press-publications/press-news/blog/gdpr-three-year-old-who-must-still-learn-walk-it-runs_en>.

its role of "consistency gatekeepers"[1147], and actively engage with national DPAs developing new tools to foster dynamic cooperation and issuing clearer guidance to streamline the cooperation efforts.

Finally, the complexity and size of the modern data ecosystem requires DPAs to strengthen their ranks of allies. Civil society actors are the most suited to take over this role, as it will be clarified in the next paragraph.

2.2 Enhancing the role and powers of civil society actors

The existence of a functioning network of third-party societal actors (such as NGOs, but also the media, academia and independent experts) is an essential component of the "architecture of empowerment". They allow supervisory authorities to outsource their oversight functions and create a decentralized monitoring system that alleviates the supervisory pressure borne by DPAs, enabling better detection of non-compliant behaviours[1148].

The concrete support that civil society organizations offer to ensure data protection compliance has been publicly recognized by data protection authorities. The EDPS, Wiewiórowski stated that «data protection authorities and non-governmental organizations are natural allies when it comes to putting data protection principles to practice, empowering individuals to assert their rights and holding data controllers accountable for their actions»[1149].

Yet, there is still little endorsement around the critical role that these actors play in the establishment of an efficient "fire alarm" system[1150]. By monitoring controllers'

[1147] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 193.
[1148] Woojeong Jang and Abraham L Newman, 'Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation *' [2021] JCMS: Journal of Common Market Studies jcms.13215, 2.
[1149] Wojciech Wiewiórowski, 'Civil Society Organisations as Natural Allies of the Data Protection Authorities | European Data Protection Supervisor' (15 May 2018) <https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_de>.
[1150] In the context of US public law, the term "fire alarm" was employed by Mc Cubbins and Schwartz in contrast to the term "police patrols" to identify two oversight strategies of Congress on the action of the executive branch: the former characterized by a selective monitoring, triggered by complaints from citizens and interest groups who bring potential problems to the legislators' attention; the latter involving a centralized, active and direct monitoring of the legislator to detect problems during implementation. Mathew D McCubbins and Thomas Schwartz, 'Congressional Oversight Overlooked: Police Patrols versus Fire Alarms' (1984) 28 American Journal of Political Science 165.
Jang and Newman take the concept of "fire alarm" and adapt it to the data protection field to support the advantages of a decentralized monitoring mechanisms, since they note «the standard GDPR critique mirrors earlier work on regulatory failure, which stressed the complexity of monitoring and enforcing public law». Jang and Newman (n 1148) 4.

compliance across different sectors of the society and notifying the DPA (i.e., “pull a fire alarm”) when they detect non-compliance, NGOs and other third-party actors serve as web of tripwires to signal regulatory failures. Although the individual exercise of data subjects’ rights already creates a similar distributed-control mechanism[1151], the information and power deficiencies that experience individuals acting in isolation and the focus each of those has on her peculiar interests greatly undermines the power and incisiveness of the mechanism itself. Only by relying on actors with an adequate level of expertise and a solid support structure behind them, the “fire alarm” system is able to perform its monitoring function correctly and effectively, without being adversely affected by the complexities of the data governance reality.

Such a distributed-control model of third-party societal actors is extremely valuable, especially when supervisory authorities have limited resources, like in the case of DPAs.

On the one hand, it creates bottom-up channels of information, which bolster the oversight capacity of the overall system, improving detection of non-compliant behaviours, quicker and more intense enforcement actions. At the same time, these actors complement the educational tasks of DPAs, helping to raise awareness and heightening public pressure on the most sensitive social issues[1152].

On the other hand, the establishment of this European collective network stimulates partnerships among societal actors located in multiple states, which enhance the cross-border dimension of data protection enforcement and help to compensate the still unsatisfactory transnational efforts of national DPAs. As noticed, the fact that NGOs, the media or academics are not bound to any specific national electorate and that do not face the same regulatory constraints of supervisory authorities enables them to mobilize campaigns and promote their actions across member states[1153]. These joined efforts in multi-jurisdictional activities extend the scope of decentralized monitoring and enable the detection of «systematic non-compliance even when the evidence is dispersed across multiple states»[1154].

[1151] As noted by Rodotà and mentioned above, under Chapter III, par. 4.
[1152] See in more detail below, par. 2.2.2.
[1153] Jang and Newman (n 1148) 6–7.
[1154] ibid 5.

The following paragraphs explore in more detail the advantages that a healthy "fire alarm" system, which includes active citizens but goes way beyond and above them, may bring.

2.2.1 Better scrutiny, understanding and detection

To have a wide array of civil society actors that offer their services means, first of all, to dispose of an army of eyes and ears ready to investigate controllers' behaviours in the context of data processing.

To perform these monitoring and supervisory functions, NGOs, journalists and researches have devised a number of successful strategies[1155]. These entities, for example, can establish a "collaborative relationship" with controllers and obtain, with their agreement, information useful to investigate how processing activities are conducted in practice. This is the case, more common in the academic research contexts, of the conclusion of voluntary data sharing agreements[1156], based on which controllers consent to share a number of information with researchers upon their request. Clearly, because these instruments entail controllers' collaboration, they usually provide a limited and high-level oversight of systems' functioning, since they remain at the mercy of controllers' preferences[1157].

More effective to exercise an unbiased control appear to be approaches that do not depend on the willingness of the data controller to share data or access to their systems.

2.2.1.1 Technology monitoring

The use of independent tools, like scraping software or other interception techniques, that provide access to useful data otherwise sealed-off by private entities[1158], have been effectively used by these entities to gain better insights into data processing. These tools can range from more intrusive traffic monitoring programs to browser plugins that

[1155] See extensively in Jef Ausloos and Michael Veale, 'Researching with Data Rights' [2021] Technology and Regulation 136.
[1156] E.g., the Facebook's initiative to help scholars assess social media impacts on elections. 'Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections' (*Meta*, 9 April 2018) <https://about.fb.com/news/2018/04/new-elections-initiative/> accessed 1 November 2021.
[1157] As demonstrated by the difficulty for researchers to retrieve the promised data in the Facebook case above, and other similar. Camilla Hodgson, 'Facebook given Deadline to Share Data for Research' *Financial Times* (28 August 2019) <https://www.ft.com/content/147eddec-c916-11e9-af46-b09e8bfe60c0> accessed 1 November 2021; Axel Bruns, 'After the "APIcalypse": Social Media Platforms and Their Fight against Critical Scholarly Research' (2019) 22 Information, Communication & Society 1544, 1550.
[1158] Ausloos and Veale (n 1155) 139.

control browser or social media activity [1159], which help researchers and activists to independently monitor and compare applications' data consumptions and unmask their functioning. The "Website Evidence Collector"[1160] developed by the EDPS is one of the automated tools that allows to gather evidence on personal data processing operations of websites, without website owners' having to give any permission of sort.

A major issue with these instruments is that they suffer from rapid technological changes in controller's infrastructures (operating systems, web browsers, apps), that make them useless very quickly, and their lawful use is limited by the hurdles of complying with legal requirements, including data protection ones[1161].

2.2.1.2 Use of data subjects' rights

A particularly innovative approach adopted by NGOs and other actors to monitor controllers' activities involves a tactical use of data subjects' rights[1162].

(i) EFFECTIVE EXERCISE OF DATA SUBJECTS' RIGHTS – One of the issues individuals experience when trying to "control" their personal data is that controllers do not put them in the conditions to exercise it effectively.

NGOs can therefore make "use" and exploit some of the characteristics of individual GDPR rights to assess whether controllers are complying with them and are not obstructing or manipulating their exercise. For example, relying on the transparency obligations set forth under Articles 13-14 GDPR, NGOs have access to a number of contents (provided through "privacy policies") that if read carefully and understood (which data subjects usually don't) can already provide an insight into controllers' processing practices. Although these documents are usually crafted carefully, possibly in abstract and general terms, this information may be enough for an experienced reader to discover discrepancies and lack of necessary information[1163], or even more frequently, improper formulation of consent forms and deceptive collection of data

[1159] Ausloos mentions a number of these instruments, such as WhoTargetsMe (https://whotargets.me/en/) or Algorithms Exposed (https://algorithms.exposed) or the now exhausted project DatenSpende (https://datenspende.algorithmwatch.org). ibid.
[1160] This is an open source software tool that supports the automated privacy and personal data protection inspection of websites, European Data Protection Supervisor, 'EDPS Inspection Software' <https://edps.europa.eu/edps-inspection-software_en> accessed 1 November 2021.
[1161] Ausloos and Veale (n 1155) 139–140.
[1162] Mahieu and Ausloos (n 1079) 3 ff.; Ausloos and Veale (n 1155) 144 ff.
[1163] See e.g., Alfredo J Perez, Sherali Zeadally and Jonathan Cochran, 'A Review and an Empirical Analysis of Privacy Policy and Notices for Consumer Internet of Things' (2018) 1 Security and Privacy; Dimitra Kamarinou, Christopher Millard and W Kuan Hon, 'Cloud Privacy: An Empirical Study of 20 Cloud Providers' Terms and Privacy Policies—Part I: Table A1' (2016) 6 International Data Privacy Law 79.

subjects' consent[1164]. Alternatively, NGOs can craftily replace data subjects in the exercise of certain individual rights (usually those that require a pro-active request) on their behalf and, by this way, check the level of quality and accuracy of controllers in the handling and follow up of the sent requests. In this sense, investigations on how companies responded to requests of data portability[1165] and access[1166] helped to uncover systemic shortcomings in the responses' rates and contents, which in turn may lead to spotlight underlying inconsistencies in data processing and trigger further scrutiny in the controllers' activities.

(ii) *SCRUTINIZE CONTROLLERS' PROCESSING ACTIVITIES* – Even though individuals are provided with instruments, such as the "right to access", that allow them to exercise a deeper scrutiny on controllers' activities regarding their personal data, they may lack the time and skills to take fully advantage of it.

Here, again, NGOs and other activists have stepped in, coming up with successful strategies to use the right to access of data subjects to gain a better insight into controllers' systems and investigate, review, and expose how personal data is being processed[1167]. The right to access is typically considered an essential tool to enable data subjects to exercise their other GDPR rights (e.g., erasure or rectification). However, when contextualized in a broader "architecture of empowerment", its value extends beyond the individual himself. As Mahieu et al. state, despite being structured as an individual right, it «plays a pivotal role in collective efforts to overcome information asymmetries»[1168] where «the benefit is meant to be for the society as a whole»[1169]. NGOs, activists and journalists in fact have started to use this right to access, with the purpose to benefit the whole community, by collect findings on controllers' misbehaviours and publicly sharing them to raise awareness[1170] and force compliance.

[1164] Based on the analysis of the "accept" buttons of cookie banners, NOYB filed 422 complaints for violation of consent requirements. NOYB, 'Noyb Files 422 Formal GDPR Complaints on Nerve-Wrecking "Cookie Banners"' (*noyb.eu*) <https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners> accessed 2 November 2021.
[1165] See e.g., Wong and Henderson (n 790).
[1166] See Mahieu, Asghari and van Eeten (n 789); Ausloos and Dewitte (n 789); NOYB, 'Netflix, Spotify & YouTube: Eight Strategic Complaints Filed on "Right to Access"' (*noyb.eu*) <https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access> accessed 1 November 2021.
[1167] Art. 15 GDPR ("Right to access of the data subject").
[1168] Mahieu and Ausloos (n 1079) 16.
[1169] Mahieu, Asghari and van Eeten (n 789) 16.
[1170] For example, Prof. Veale exercised his right to access to understand what Netflix was collecting when watching "Bandersnatch", an interactive episode of the famous "Blackmirror" series that allows viewers to make decisions for the main character. Michael Veale, 'Netflix Claim They Only Use Individual Choices to

In some cases, the right has been exercised in a "isolated" manner but has led to results that benefitted the entire community of data subjects. This is usually the case when an activist or a journalist makes an access request on his own behalf (therefore limited to his specific situation), but then uses the retrieved information to trigger actions or raise awareness that help to protect an entire community of concerned individuals. The "*Schrems vs. Facebook*"[1171] saga, triggered by an access request submitted by the Austrian activist Max Schrems and resulting in one of the most important CJEU decisions in data protection history, to the benefit of millions of EU citizens, is probably the most representative examples in this sense.

Some of the most interesting cases, however, have seen NGOs and other researchers employing the right to access in a "collective manner"[1172], namely through the planned and strategic submission of multiple access requests by different data subjects, which result in the collection of a large volume of responses. Several authors have underlined the merits of this "collective" approach at least under two aspects. First, when this right is used in a collective manner, «it creates a context to judge the quality of replies and the lawfulness of the data practices by comparing replies to similar access requests»[1173]. Further, participants involved in these collective projects «perceive a societal much more than an individual value in exercising this right, not the least because through collective use, the power imbalance between individual citizens and organisations shifts in favour of the citizen»[1174].

Practical cases of NGOs or academics using the right to access following this "collective approach" are abundant. The digital rights organization Privacy International, for example, has made use on several occasion of this access modality to have a better understanding of the ways in which personal data was processed by companies in the

Inform Which Video Segments to Show, Although They Do Learn from Aggregate Choices, as Would Be Expected' (12 February 2019) <https://twitter.com/mikarv/status/1095110950028562433>. See further below.

[1171] In 2011, Max Schrems (a then Phd candidate) submitted an access request to Facebook to know the information the company held about him. Following the response, he submitted 22 complaints at the Irish DC for violations of data protection rules (http://europe-v-facebook.org/EN/Complaints/complaints.html). Although most of the claims were withdrawn, some of them resulted in the famous "Schrems I" decision, where the CJEU declared invalid the then EU-US adequacy decision (Safe Harbor) for the transfer of personal data in the US, CJEU Judgement of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650. This in turn triggered the "Schrems II" decision, where the CJEU once again invalidated the new EU-US adequacy decision (Privacy Shield) and provided further clarifications on standard contractual clauses. CJEU Judgement of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559.

[1172] Mahieu and Ausloos (n 1079); Ausloos and Veale (n 1155); Ausloos and Dewitte (n 789); Mahieu, Asghari and van Eeten (n 789).

[1173] Mahieu, Asghari and van Eeten (n 789) 17.

[1174] ibid.

data broker and credit-referencing industries[1175] or to dive deeper into Twitter's sharing practices[1176], producing worrying but extremely helpful revelations on companies' wrongdoings. In a similar vein, another human rights foundation, Panoptykon, has conducted several investigations on real-time bidding advertising practices by sending access requests to various companies involved in the AdTech ecosystem[1177]. In other cases, the right has been employed by labour rights movements in the platform economy to get insight on the employers' processing activities that could negatively affect labour rights. Worker Info Exchange, for example, has organized campaigns to incentivize workers of the gig economy to use their access rights with their employers' platforms (e.g., Uber, Deliveroo, Ola) and share the results with the NGO to facilitate targeted investigations on how performance algorithms were employed to profile workers[1178]. Another example is the "OPENSchufa" project[1179] launched by two NGOs, Algorithm Watch and Open Knowledge Foundation Deutschland, to understand the functioning of the credit scoring algorithm used by the German credit agency Schufa and demand transparency and fairness on its employment[1180]. Finally, many initiatives of this kind have been carried out in the fields of price discrimination and political micro-targeting. Bits of Freedom sent subject access requests to various organizations, such as online stores, travel agencies and insurance companies, to understand how personal data were used by companies to profile customers, leading to personalized pricing[1181]. While, Open Rights Group started a campaign calling on the general public to submit

[1175] Privacy International, 'Tell Companies to Stop Exploiting Your Data! | Privacy International' (*privacyinternational.org*, 8 November 2018) <https://privacyinternational.org/campaigns/take-control-your-data> accessed 2 November 2021.
[1176] Privacy International, 'What Does Twitter Know about Its Users? #NOLOGS' (*privacyinternational.org*, 16 February 2012) <http://privacyinternational.org/blog/1504/what-does-twitter-know-about-its-users-nologs> accessed 2 November 2021.
[1177] Panoptykon Foundation, 'Panoptykon Files Complaints against Google and IAB Europe' (*panoptykon.org*, 28 January 2019) <https://en.panoptykon.org/complaints-Google-IAB> accessed 2 November 2021.
[1178] Worker Info Exchange, 'Data Rights for Digital Workers' (*workerinfoexchange.org*) <https://www.workerinfoexchange.org> accessed 2 November 2021; App Drivers and Courier Unions, 'Collective Action Campaign to Claim Your Data from Uber' <https://www.adcu.org.uk/wie> accessed 2 November 2021. Some of these initiatives have triggered collective legal actions against Uber and Ola, that resulted in groundbreaking decisions that ordered the two platforms to provide transparency and reveal specific information on the systems and algorithms used in the management of drivers' performances. Worker Info Exchange, 'Gig Workers Score Historic Digital Rights Victory against Uber & Ola' (*workerinfoexchange.org*) <https://www.workerinfoexchange.org/post/gig-workers-score-historic-digital-rights-victory-against-uber-ola-2> accessed 2 November 2021.
[1179] Algorithmic Watch, Open Knowledge Foundation Deutschland (n 712).
[1180] The campaign was able to motivate more than 4,000 people to provide their SCHUFA information gathered through 30,000 access requests submitted to SCHUFA. The data were made available to journalists from Der Spiegel and Bayerischer Rundfunk for a data-journalism investigation.
[1181] Mahieu and Ausloos (n 1079) 27.

subject access requests to UK political parties in order to determine how political parties use voters' personal data by political parties to profile voters[1182].

This brief overview demonstrated how activists, journalists and NGOs are well equipped to initiate strategic actions that aim at scrutinize and challenge emerging data practices governing our society, which would not be possibly achieved by average individual subjects acting alone. This scrutiny activity carried out by these actors is essential to raise awareness and public pressure on discovered issues and/or activate redress mechanisms to pursue better compliance[1183].

2.2.1.3 Barriers to effective scrutiny, understanding and detection

Against evident benefits, these investigation practices, especially when exercised in a collective manner, face a fair share of challenges.

The main one concerns the modalities of exercise. The right to access, in fact, is designed for *individuals*, namely only the data subject can request access to his/her personal information. To exercise the right in a collective manner, NGOs and researchers normally need to recruit participants that have existing relations with data controllers (companies and organizations) of interest to their study[1184]. The process is not unworkable, as the many success stories above testify. However, it suffers major scaling limitations and may require quite an effort especially for unexperienced participants, who would find themselves burdened to follow up on the request process. As opposed to this standard process, it has been recently proposed as an alternative solution a "delegated access" method, according to which participants sign a delegation form that enables researchers/NGOs to act on their behalf during the access request process[1185]. Although the GDPR does not expressly provide for the exercise of access

[1182] Open Rights Group, 'Who Do Political Parties Think We Are?' (*action.openrightsgroup.org*) <https://action.openrightsgroup.org/who-do-political-parties-think-we-are-4> accessed 2 November 2021. Other initiatives were pursued on an individual basis, by journalists and academics, especially in the context of the Cambridge Analytica scandal. See for example Carole Cadwalladr, 'UK Regulator Orders Cambridge Analytica to Release Data on US Voter' *The Guardian* (5 May 2018) <https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-uk-regulator-release-data-us-voter-david-carroll> accessed 2 November 2021.

[1183] See below par. 2.2.2.

[1184] Hadi Asghari, Thomas van Biemen and Martijn Warnier, 'Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests' [2021] arXiv:2106.06844 [cs].

[1185] Hadi Asghari, Thomas van Biemen and Martijn Warnier, 'Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests' [2021] Proceedings of the The 5th Workshop on Technology and Consumer Protection (ConPro'21), IEEE, 2021. 2–4 <http://arxiv.org/abs/2106.06844> accessed 2 November 2021.

rights through third parties[1186], it does also neither explicitly prevent it[1187]. The ultimate goal of this approach is to create a win-win collaboration between data subjects and researchers, whereby the former can make use of the researchers' skills and experience and leave them navigate the bureaucratic hurdles of the access process; the latter can file access requests in bulk on behalf of hundreds of subjects and gain access to a bigger pool of data without having to rely on each individuals' proactivity[1188]. When tested in practice, yet, the delegated access model has clashed with the current mistrust of data controllers to accept proxies as valid documents to provide data subjects' information to a different subject[1189]. To be effective, the approach requires further refinement. Institutional recognition of the legitimacy of this practice and greater use by academics and digital rights activists will help to increase its acceptance among controllers.

With a view to overcome these difficulties, some authors have even suggested the introduction of a new category of privacy rights for NGOs, that they would be allowed to exercise in the collective interest[1190], without the need to rely on the escamotage of individuals' mandate[1191]. These could include rights (e.g., to access or explanation of automated-decisions) that serve the purpose of transparency, but also reaction rights (e.g., right to block certain processing) that, without overrunning individuals' agency, may be used to prevent dangerous activities to continue without additional investigation or adequate information to individuals. The provision of substantive autonomous rights to representative organizations, exercised in the broader collective interest, would lead to a fundamental reorganization of the power dynamics among the actors involved in

[1186] In the GDPR, representation of data subjects is recognized in other articles, like Art. 35 GDPR, where in the context of the data protection impact assessment the controller, where appropriate, has to «seek the views of data subjects *or their representatives* on the intended processing», or under Art. 80 GDPR, which establishes the right to mandate representative organizations to lodge complaints before a DPA or a court.

[1187] As Asghari et al. highlights, the exercise of legal actions on one's behalf is a well-established practice in Western legal systems. Asghari, van Biemen and Warnier (n 1185) 2. In addition, the possibility for data subjects to mandate associations and organizations to exercise data protection rights on their behalf was already included in certain national data protection laws, before the adoption of the GDPR, see for example Art. 9(2) of the old Italian Privacy Code.

[1188] ibid 2–3.

[1189] ibid 4–7.

[1190] Mantelero, 'La Privacy All'epoca Dei Big Data' (n 690) 1204–1205; Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017) 149.

[1191] This possibility is partially envisaged by the GDPR under Art. 80(2) GDPR, which however limits the exercise to a number of "procedural rights", namely the right to lodge a complaint before a supervisory authority or start legal action without, independently of a data subject's mandate, if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing».

the governance of personal data, adding alongside data subjects a further class of entities able to autonomously interface with data controllers. However, it would also determine a structural change in the data protection framework that would necessarily open a bigger discussion on the contended topic of "group privacy rights"[1192], namely the possibility for legal entities and groups to be right holders in the data protection domain. Recent works on group privacy have underlined the current difficulties of conceptualizing such notion and the careful balancing of conflicting interests that the introduction of a new class of group or collective rights would require in practice[1193]. This suggests that the road for NGOs to exercise GDPR-like rights in the collective interest is long and uphill.

A further set of challenges, which more broadly affect the efficiency of the right to access itself, concerns the legal and technical issues that may brought up by controllers to obstacle the investigatory attempts of civil society actors. In particular, obstructions of controllers on the basis of conflicting interests (e.g., privacy of third parties or controllers' IP rights); existence of national exemptions in the exercise of subjective

[1192] "Group privacy" is a very heterogeneous concept that has been used with a variety of meanings and applications. In early US literature, the term was employed as an extension of individual privacy to emphasize either the capacity of groups to determine themselves the use and disclosure of information about them ("organizationl privacy", Alan Westin, 'Privacy And Freedom' (1968) 25 Washington and Lee Law Review 166 <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>.) or the aggregate interest of intimacy concerning the information shared within a group ("relational privacy", Edward J Bloustein, *Individual and Group Privacy* (Transaction Books 1978) 125.). In Europe, despite not referring to the concept of group privacy, the provision of a right to data protection for recognized legal entities (corporations, associations and other recognized organizations) was introduced in a number of national statues (Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland) Bygrave (n 14) 173 ff. The approach was later abandoned in favour of a view of data protection as intrinsically linked to individual values that only natural persons could claim. More recently, some authors have tried to revive the debate on the concept of "group privacy", presenting it as a possible solution to the group and collective impacts of data processing as a result of big data analytics and advanced profiling activities, that lead data-driven decisions to be based on and increasingly affect larger groups rather than single individuals. In their view, introducing "group privacy" rights would provide affected collectivities (socially recognized, such as minorities, political activists and NGOs, but also new "big data" derived groups) the means to control, as a collective, personal data belonging to their community and, in this way, acting autonomously to protect the collective data protection interests of the group *qua* group. See Luciano Floridi, 'Group Privacy: A Defence and an Interpretation'; Lanah Kammourieh et al, 'Group Privacy in the Age of Big Data'; Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New DimensionSee of Privacy and Data Protection in the Big Data Era' and Ugo Pagallo, 'The Group, the Private, and the Individual: A New Level of Data Protection?', all in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017).

[1193] See in particular Kammourieh and et. al (n 1192); Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' (n 1190); Pagallo (n 1192).

rights and lack of technical tools to provide users with effective access to the requested information may also severely curtail the scrutiny efforts of NGOs and academics[1194].

2.2.2 Raise awareness and public pressure

Another important function of civil society actors is to galvanize the attention on the most pressing societal issues, raise public awareness and generate mobilizing effects[1195].

2.2.2.1 Educational function

Awareness campaigns on data protection-related topics are a common tool used mostly by digital rights NGOs to educate and inform people on important issues and topic in the data protection arena, usually connected to companies' controversial, dangerous or unlawful data processing. These educational contents can take the form of reports and publications, as a by-product of NGOs' research and supervisory activities[1196], but can also be provided in a more appealing form, through video contents; graphic images and posters[1197] that may attract the attention of a broader public.

2.2.2.2 Mobilization and public pressure

Beside educational purposes, awareness campaigns are essential for NGOs to generate mobilizing effects to engage the collectivity. Investigatory activities realized with the use of collective access rights, like the examples above illustrated, are generally preceded by outreach campaigns advertised by interested NGOs to galvanize public attention and solicit citizens' participation, which are critical for the successful outcome of the collective action[1198].

Further, awareness campaigns can be exploited to generate momentum and put pressure on DPAs to accelerate and follow-up on complaint-led investigations[1199]. In 2018, La Quadrature du Net filed on behalf of 12.000 people a number of complaints before the CNIL (the French Data Protection Authority) against Google, Apple,

[1194] See extensively in Ausloos and Veale (n 1155) 149–152.
[1195] Jang and Newman (n 1148) 9–10.
[1196] To name just a few, EDRi (https://edri.org/what-we-do/publications/), Privacy International (https://privacyinternational.org/search-campaign?search_api_fulltext=&f%5B0%5D=topic%3A90), and NOYB (https://noyb.eu/en/projects) are particularly active in the field.
[1197] For example, to promote their call for donations in support of the collective actions against the big 5 (Google, Apple, Facebook, Amazon, Microsoft, "GAFAM"), La Quadrature du Net, a French-based NGO, advertised a very successful GAFAM poster campaign, https://gafam.info/ .
[1198] See notes 1175-1180 above.
[1199] Jang and Newman (n 1148) 10.

Facebook, Amazon and Microsoft[1200], that would have hardly been possible without the effective mobilizing campaign launched by the organization[1201]. The same kind of public awareness and pressure can be generated by the media exposure of relevant topics or issues, thanks to the hard work of investigative journalists. For example, investigations carried out by front-line press journalists have helped to uncover and bring under the public eye the impacts of algorithmic matching and "desirability scores" in online dating apps (e.g., Tinder)[1202], the data collection strategies behind mobile games (Wizard Unite)[1203] or the type of data Amazon was storing with its devices (Ring Doorbel)[1204]. These contributions help to guide the limited resources of formal enforcement bodies in the right direction[1205].

In addition, the public pressure generated by an active press, NGOs campaigns and mobilized citizens can be a powerful incentive for controllers as well to take action and correct uncompliant behaviours.

2.2.3 Concluding remarks

NGOs and other societal actors engaged in the data protection field are a critical resource in our society. They allow to create a network of operators that takes the responsibility to carry out certain monitoring functions, traditionally exercised by supervisory authorities or individual subjects. This decentralization helps to extend the range, scope and intensity of supervision. It supports data subjects in identifying and opposing to situations in which controllers do not handle their individuals' rights and requests correctly, hindering their ability to act meaningfully and effectively in the management of their personal data. Even more significantly, the investigative work performed by these organizations helps to increase the exposure of the dangers of processing practices, both for individual and society, often hidden behind obscure, manipulative or extremely complex data uses.

[1200] La Quadrature du Net, 'First Sanction against Google Following Our Collective Complaints' (*laquadrature.net*, 21 January 2019) <https://www.laquadrature.net/en/2019/01/21/first-sanction-against-google-following-our-collective-complaints/> accessed 2 November 2021. This

[1201] See note 1197.

[1202] Judith Duportail, 'I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets' *The Guardian* (26 September 2017) <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold> accessed 2 November 2021.

[1203] Cecilia D'Anastasio and Dhruv Mehrotra, 'The Creators Of Pokémon Go Mapped The World. Now They're Mapping You' (*Kotaku*) <https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714> accessed 11 January 2022.

[1204] Leo Kelion, 'Amazon's Ring Logs Every Doorbell Press and App Action' *BBC News* (4 March 2020) <https://www.bbc.com/news/technology-51709247> accessed 2 November 2021.

[1205] Mahieu and Ausloos (n 1079) 11.

At the same time, NGOs, journalists and academics, with their expertise, broad vision and outreach, are best placed to raise awareness on the most pressing data protection issues, turning the spotlight on the unnoticed or hidden threats that data practices may entail.

In particular, the awareness and mobilizing activities in which NGOs and the media are engaged are fundamental tools that serve many different purposes. They help to educate people and make them more conscious about the processing environment that surrounds them, which is a necessary pre-condition for individuals to exercise effective control on their personal data. Acting as a filter, NGOs and the other society actors select and investigate on specific type of processing, activities or controllers, that are usually the more socially significant and dangerous, and produce accessible explanations, in this way helping citizens to channel their limited attention on a selected number of cases and digest the information more easily. Since the media and public attention raised on data protection topics can trigger DPAs' investigations, legal claims and produce direct reputational damages, these activities are valuable deterrents to refrain them from persevering in uncompliant behaviours.

As highlighted above, there are however still many barriers that undermine the effective actions of NGOs and other societal actors.

NGOs and other societal actors had to come up with innovative ways to perform their investigatory tasks, exploiting the leeway left by a fundamentally individual rights-based system, which however risks to create significant obstacles to their activity. To strengthen the monitoring role of NGOs, a more viable alternative requires supervisory authorities and other institutional bodies to support the initiatives of these organizations and other societal actors in stronger terms, publicly legitimizing their actions and following up on their reports with formal investigation and sanctioning procedures.

In the same way, in relation to awareness and educational activities, while NGOs and other actors are already active in this field, their initiatives should be given broader resonance and brought to the attention of a larger public. Supervisory authorities and other institutional bodies, equally engaged in educating citizens on data protection matters, should collaborate more intensely with these actors, to converge the energies on specific initiatives and create a bigger platform to increase their visibility.

3 Collective management of personal data

Data subjects, when considered individually, are often in a disadvantage position compared to controllers, in terms of knowledge, resources and power to exercise their rights. This often places them in a weaker position to exercise effective control on their personal data. To empower data subjects and overcome the limits of an individualized control model, a viable option could be the introduction of "intermediaries", that could take up the management of subjective rights, in the interest and on behalf of data subjects, entering into the traditional one-to-one relationship between data subjects and controllers, to the advantage of the former.

This type of approach has been adopted by some emerging data governance models, pioneered in recent years, that move away from an unrealistic paradigm of "individual self-management" and experiment to leverage the synergies resulting from collective forms of management of personal data.

3.1 Collective Consent

Already back in 2010, Bygrave and Schartum advanced a proposal for a sort of collective management model, mainly built around the notion of "collective consent"[1206]. The term was used to denote a type of consent that was «exercised on behalf of a group of data subjects but without these persons individually approving each specific exercise of that decisional competence»[1207]. Based on this proposal, data subjects would transfer the exercise of their decisional competences to a third-party organization, which in turn would take decisions on behalf of all the delegating members. In other words, the conferral or withdrawal of consent would be binding on all of the group members, even when some of them disagreed with a particular decision. For the mechanism to work properly and in compliance with data protection requirements, the authors included a number of basic safeguards. First, collective consent was best established where individuals were already structured in groups that shared a set of common interests (e.g., in trade unions, environmental associations, sport clubs or student associations) [1208]. The purposes and values of these organizations would influence and determine how collective consent was exercised for the benefit of their associates. Secondly, collective consent needed to respect the same conditions that

[1206] Bygrave and Schartum (n 673).
[1207] ibid 169.
[1208] ibid 169–170.

data protection law prescribed for individual consent[1209]. Hence, individuals had to be free to provide (or withdraw) the transfer of competence to the organization without any detrimental consequence (e.g., exclusion from the organization), and retain individual decision-making ability to exercise their preferences at odds with the decision adopted by the organization[1210]. According to the authors, this mechanism would bring a number of benefits. The intermediation of an experienced and qualified organization, in fact, would ensure that privacy-related interests of data subjects were administered more carefully. These middlemen-entities could have the skills and resources to assess with greater awareness the advantages and disadvantages, especially in a long-term perspective, of a given processing[1211]. At the same time, the mechanism would mitigate the power imbalances that affect individual decision-making. Representing a large group of data subjects, these organizations would in fact have stronger negotiating powers that would enable them to put data controllers under more pressure, making the bargaining process on data processing conditions tougher[1212].

Recently, other authors have praised the possible advantages of collectivizing consent and in general the management of "data rights" to tackle the power imbalances of the digitized society[1213]. They are however less specific with regards to the requirements that this type of mechanism should meet in practice (e.g., identification of the collective members, the modalities of the decision-making process) that are left open to further research[1214].

3.2 Data Trusts and Data Cooperatives

The intuition of Bygrave and Schartum seems to have been taken up by proposals of new "data governance models" that are supporting a collective approach to personal data management.

[1209] In particular, explicitness, voluntariness and revocability, along with the other requirements for a valid consent carefully detailed under Articles 4(11) and 7 GDPR, as well as in the Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 436).
[1210] Bygrave and Schartum (n 673) 170.
[1211] ibid 171.
[1212] ibid 171–172.
[1213] See e.g. Anouk Ruhaak, 'When One Affects Many: The Case For Collective Consent' [2020] Mozilla Foundation <https://foundation.mozilla.org/en/blog/when-one-affects-many-case-collective-consent/> accessed 9 November 2021.
[1214] ibid.

Currently, the GDPR framework, which is inspired by an individual right-based ideology[1215] adopts a "personal data sovereignty model"[1216], according to which data subjects only and individually are provided with the instruments to control who access, use and shares their personal data. The same approach underlies the privacy-friendly technologies (e.g., personal data stores and similar) examined in the previous chapter, which move along the lines of an individualized control logic by providing data subjects with the technical means to facilitate and automate the micro-management of their individual privacy preferences.

More recently, however, proposals for new models of data governance have started to place more emphasis on the role that intermediaries may play when interposed in the traditional one-to-one relationship between user (data subject) and big platforms (controllers).

It should be pointed out that these models have not developed with data protection objectives in mind, rather with the objective of tearing down the quasi data-monopolies created by the platform society and democratize the access to data, with a view to redistribute the value that data generate[1217]. Although "value-distribution" remains often their primary goal, the mechanisms adopted by these governance models to achieve this result have ultimately the effect of bringing control on personal data back to the data subjects' "side", thus ultimately supporting the data protection cause.

These mechanisms, in fact, provide that personal data and related rights are managed on behalf of data subjects (entirely or in a shared manner) by a third entity with more expertise and skills, which in turn can take advantage from the "collective" management of data of multiple data subjects to gain a stronger negotiating power vis-à-vis data controllers that wish to access and use this data[1218]. Two of the models sharing these

[1215] Kieron O'hara, *Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship* (University of Southampton 2019) 8.
[1216] This is how Micheli and others define the governance model characterized by data subjects retaining most of the control on their data, both in terms of privacy management and data portability. Marina Micheli and others, 'Emerging Models of Data Governance in the Age of Datafication' (2020) 7 Big Data & Society 205395172094808, 9.
[1217] ibid 1–2. Ada Lovelace Institute - UK AI Council, 'Exploring Legal Mechanisms for Data Stewardship - Chapter 1 Data Trusts' (Ada Lovelace Institute - UK AI Council 2021) 17 ff. <https://www.adalovelaceinstitute.org/feature/data-trusts/#fnref-6>.
[1218] Although from a GDPR standpoint these intermediaries may qualify as data controllers or data processors, depending on how their services and their relationship with the data subject is framed, in this paragraph "data controllers" is used only to identify those end-operators that are interested in collecting and using data subjects' personal data for their own specific purposes.

characteristics are "data trusts" and "data cooperatives"[1219], that will be briefly presented below.

(i) DATA TRUST - A "data trust" is defined as a legal structure that provides independent stewardship of data[1220]. Data trusts are created when individuals hand over their data, along with their data rights, to a "trustee" (a person or an organization) that has a fiduciary duty to steward them in the sole interest of the group of beneficiaries and never in its own self-interest[1221]. These constructs essentially take the legal concept of trust, traditionally used in common law systems to hold and make decisions about specific assets by establishing a fiduciary relationship between trustee and trustor, and apply it to data[1222]. Therefore, from a data protection perspective, data subjects would qualify as both trustors and beneficiaries of the trust, who would delegate to the trustee the exercise of the subjective rights (Art. 15-22 GDPR) and decisional competences (exercise of consent for data processing) established by the GDPR, on their behalf and in their interest[1223]. Data trusts create a vehicle for individuals «to state their aspirations for data use and mandate a trustee to pursue these aspirations»[1224]. This structure, that intermediates between data subjects and controllers, may help protecting individual rights. The trustee acts within the limits of the purposes specified in the trust's founding documents, that are accepted by the individuals at the moment of conferral[1225]. To ensure individuals are involved in the bigger scheme of decision-making, mechanisms for deliberation or consultation with beneficiaries may also be built into a trust's founding

[1219]For an overview of the different data governance approaches that are emerging in literature and in practice, see Jonathan Van Geuns and Ana Brandusescu, 'What Does It Mean? | Shifting Power Through Data Governance' (Mozilla Foundation 2020) <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/> accessed 9 November 2021; Micheli and others (n 1216).

[1220] Open Data Institute, 'Defining a "Data Trust"' (Open Data Institute 2018) <https://theodi.org/article/defining-a-data-trust/> accessed 9 November 2021.

[1221] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' [2019] International Data Privacy Law ipz014, 240; Van Geuns and Brandusescu (n 1219) 13.

[1222] Open Data Institute (n 1220). There is an open discussion on whether a data trust may take the form of a "true" trust Delacroix and Lawrence (n 1221) 242. or would rather only take legal trusts as inspiration for a certain type of hands-off arrangement involving fiduciary duties. O'hara (n 1215) 24.

[1223] Data trust is a governance model that may serve different situations, that do not necessarily involve personal data (but may also concern non-personal data) or data subjects as trustor and beneficiaries (a trust may be created by organizations or other actors in relation to other data rights established by law on the information they hold). O'hara (n 1215) 21. From a data protection perspective, however, "bottom up" data trusts, where personal data are managed in the interest of a group of data subjects, are those of main interest. Delacroix and Lawrence (n 1221).

[1224] Ada Lovelace Institute - UK AI Council (n 1217) 34.

[1225] ibid.

charter[1226]. However, case-by-case decisions are deferred to the trustee that, in line with the beneficiaries' interests and trust's purposes, decides in practice who has access to the data and who can use it, but that has also the duty to ensure compliance with the trust's terms and terminate the relationship when data users do not respect them[1227]. The agency of individuals is not nullified. They would retain individual control in that they would agree to the terms of the trustee's mandate; maintain (or withdraw it at any moment) the "trust" in the organization; and participate in the determination of the trust's operations[1228]. At the same time, the micro-management of personal data is deferred to the trustee, that has the expertise and the negotiating strength, stemming from the collective exercise of data rights, to act in the best interests of the beneficiaries. Many legal and practical critical questions are still open to discussion[1229]. However, ideally, the fiduciary aspects and collective retain that characterizes data trusts have an interesting potential to help shifting power dynamics and protect people from vulnerabilities resulting from personal data processing[1230].

(ii) DATA COOPERATIVE - On a different albeit similar note is the phenomenon of "data cooperatives". Typically, a cooperative is formed by a group that has common interests, which are better pursued jointly than individually, also in light of the stronger bargaining power it can exercise as a collective[1231]. Regardless of the legal form that cooperatives may take, depending on the jurisdiction, key characteristics are generally: voluntary and open participation, democratic member control and pursuit of the benefits of its members[1232]. These mechanisms are now being explored in the context of data stewardship. Data cooperatives have been defined as constructs that «aim to facilitate the collaborative pooling of data by individuals or organizations for the economic, social,

[1226] In this case, the trust model would effectively function in ways similar to a cooperative, albeit with robust fiduciary duties. Delacroix and Lawrence (n 1221) 242.
[1227] Anouk Ruhaak, 'Data Trusts: Why, What and How' [2019] Algorithmic Watch <https://algorithmwatch.org/en/data-trusts-why-what-and-how/>.
[1228] Delacroix and Lawrence (n 1221) 242.
[1229] The legal framework and design of data trusts; their compatibility with the current regulatory environment (in particular data protection principles); the qualifications of trustees and the oversight mechanisms to hold them accountable; as well as the technical tools and interfaces needed to erect this structure are all issues that require further research. O'hara (n 1215) 23; Ruhaak (n 1227); Ada Lovelace Institute - UK AI Council (n 1217) Chapter 1.
[1230] Different pilot projects on data trusts have been initiated, see: https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/#what-is-a-data-trust.
[1231] Ada Lovelace Institute - UK AI Council, 'Exploring Legal Mechanisms for Data Stewardship - Chapter 2 Data Cooperatives' (Ada Lovelace Institute - UK AI Council 2021) 2 <https://www.adalovelaceinstitute.org/feature/data-trusts/#fnref-6>.
[1232] Ada Lovelace Institute - UK AI Council (n 1231).

or cultural benefit of the group»[1233]. Like data trusts, the model considers data as an asset and intends to create a structure that enables conferring members (whether individuals, organizations or other actors that hold data) to equally control and share the value of this resource, without giant market players to size all the benefits[1234]. From a data protection perspective, however, the proposal may offer an interesting opportunity for data subjects to have greater control over how their data is collected, processed and shared; and more importantly ensure that the use that is made of their data is in line with their interests. In this context, data subjects, who decided to pool their personal data together, become members of a cooperative, that they would co-own and democratically control, by actively participating in setting its policies and making decisions[1235]. To avoid that the level of individual commitment and skills implied in co-ownership and democratic control repeats the same limitations of the "individual control" model[1236], essential for the well-functioning of the cooperative would be the establishment of internal governance and consensus-building mechanisms that do not place all the decisional burden on individuals[1237]. A structure where all members vote on all possible data-sharing arrangements or data rights' exercise would easily be unviable and unscalable[1238]. On the contrary, a system that builds on a collectively agreed purpose but delegates decision-making and executive functions to a process (e.g., board, representatives) that upholds that purpose, would instead offer a way to «reduce the burden on individual members and enable the cooperative to reach decisions regarding data use and sharing»[1239].

The concept of data cooperative has surfaced also in the text of the Data Governance Act proposal ("DGA proposal") [1240], adopted in November 2020 by the EU Commission as part of the broader European Data Strategy Package. The legislative proposal aims to create a framework that facilitate data-sharing and the reuse among public and

[1233] Van Geuns and Brandusescu (n 1219).
[1234] Ada Lovelace Institute - UK AI Council (n 1231) 2. Like data trusts, also data cooperatives has as main objective that of maximizing the benefits of data uses for the members of the cooperative. Which means that, depending on the type of cooperative, members may be also SME or other actors.
[1235] Like for data trusts, the fact that the cooperative benefits its members does not mean that might not also benefit the society at large.
[1236] Julian Tait, 'The Case for Data Cooperatives' (The Data Economy Lab 2021) <https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives/> accessed 15 December 2021.
[1237] Ada Lovelace Institute - UK AI Council (n 1231).
[1238] Tait (n 1236).
[1239] ibid.
[1240] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2020) COM/2020/767 final.

private stakeholders[1241], and introduced figures named “data cooperatives” as possible new intermediaries of the digital ecosystem. They would serve individuals, by empowering them to exercise their rights under the GDPR and by ensuring oversight and transparency over the use of personal data entrusted to them. Among the tasks of data cooperatives, the DGA proposal lists the improvement of the terms and conditions offered to data subjects by data user organizations and dispute resolution affecting several data subjects within a group[1242]. The notion, however, remains extremely vague, as no clear guidance is provided on the type of legal form or organization this entity should assume[1243], nor in terms of the collective exercise of the data subjects’ rights provided under the GDPR[1244].

At the same time, the attractiveness of a cooperative approach needs to confront with a number of challenges. Apart from the issues arising from the different legal form that cooperative may take depending on the concerned jurisdiction, it remains to be seen how this governance model may comply with the current regulatory framework, in particular data protection law[1245]. Further, the establishment of the right internal governance is crucial to the success of the cooperative model, that needs to properly balance often opposite needs: streamline decision-making through delegation and centralization of certain decisional competences, but keep individual members adequately engaged and ensure they do not lose agency over their data[1246].

3.3 Concluding remarks

The idea of collective management of personal data and connected subjective rights, through the involvement of third-party intermediaries that act on behalf and in the interest of the community of data subjects they represent, has been gaining increasing traction, both at academic and institutional level, while some early initiatives have already attempted a concrete application.

For these models to become a reality a long list of issues, only briefly approached in this paragraph, needs still to be adequately researched and answered. Not the least, how

[1241] Recital 2 and 3 of the DGA Proposal.
[1242] DGA proposal, Art. 9(1)(c) and recital 24.
[1243] Julie Baloup and others, ‘White Paper on the Data Governance Act’ [2021] SSRN Electronic Journal 29 <https://www.ssrn.com/abstract=3872703> accessed 15 December 2021.
[1244] ibid 30.
[1245] Katharine Miller, ‘Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data’ (*Stanford HAI*) <https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data> accessed 15 December 2021.
[1246] Ada Lovelace Institute - UK AI Council (n 1231).

will they fit in the well-established GDPR individual-based approach. It is still unclear how a collective approach to personal data management should be designed to eschew from clashing with the traditionally individual-centric vision that underlies data protection law, whereby data subjects are individually empowered (and responsible) to exercise agency over their data. Although the GDPR expressly allows only very specific rights to be exercised by representative entities on behalf of data subjects[1247], it does not explicitly prevent data subjects to delegate third-party entities in the exercise of the other GDPR rights (Art. 15-22 GDPR). This reasoning was at the basis of the "delegated access" method developed for the collective exercise of the right to access, whose test trial, however, revealed its current practical limitations[1248]. Even more challenging may prove to justify the transfer of decision-making competences to an organization that is expected to exercise them on behalf and in the interest of an entire collectivity of data subjects. In this respect, recital 24 of the DGA proposal states «the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative», which appears to cut down the innovative potential of data cooperatives. The statement is however in conflict with the possibility, affirmed in the same proposal, for these entities to be conferred powers to «negotiate terms and conditions for data processing»[1249], which generate confusion around the relationship that these intermediaries have with respect to data subjects and other data "users". In sum, there is currently no clear guidance in terms of the collective exercise of the data subjects' rights provided under the GDPR[1250].

4 Strengthening Impact Assessment mechanisms

A framework that places great value on data subjects' self-determination, regarding whether or not to authorize certain data processing and exercise their rights, assumes individuals are capable to assess the consequences that such activities might entail. For the many reasons explored in Chapter II, it is evident how individuals are often in no position to recognize or be aware of the deeper impacts that data processing activities may produce on them and others. Not only because data processing are often overly-

[1247] In particular Art. 80(1) GDPR stipulates that representative entities may act on behalf of data subjects, when mandated by them to so do, and exercise a limited number of rights including, the right to lodge a complaint or to file a legal action.
[1248] As described under par. 2.2.1 of this Chapter.
[1249] Art. 9(2)(c) of the DGA Proposal. See also European Data Protection Board - European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (11 March 2021) 32.
[1250] Baloup and others (n 1243) 30.

complex and negative outcomes are frequently too abstract and far-away, but also due to the fact that many risks have a collective and social outreach that makes them hardly perceivable and measurable by single individuals.

The establishment of mechanisms that "outsource" the assessment of the consequences and possible risks to a more competent and informed third-party helps to overcome this deficiency and prevents that intolerable processing activities become permitted, taking advantage of data subjects' ignorance or lack of care. As discussed in the previous paragraph, the interposition of civil society actors and other "data intermediaries" in the exercise of decisional competences and subjective rights, on behalf and in the interest of data subjects, may offer a first protective shield in precluding the performance of dangerous and harmful data processing. Still, this "proxy mechanism" provides only a limited solution, as it does not lead to a generalized and preventive veto on certain processing activities. Despite the long-term systemic positive effects that such mechanism may indeed help to induce, in practice the most immediate benefits of the intermediaries' actions would be in fact enjoyed by a restricted number of subjects (those represented by the intermediary), with the risk of creating a fragmented patchwork of different "zones" of protection depending on the willingness or unwillingness of data subjects to delegate their decisions to such intermediaries[1251].

Data protection law has generally included procedures that delegate the *ex-ante* risk assessment of certain processing activities to third-party actors (e.g., supervisory authorities or controllers) different from the individual data subject. These types of assessments provide a first "creaming off" of data processing operations, as they aim to prevent the occurrence of impacts and risks, arising from the processing of personal data, that could not be adequately addressed by individuals or otherwise are contrary to the broader values of society[1252].

4.1 Early approaches to risk assessment

Since the first regulatory initiatives, data protection acts acknowledged that processing activities involved risks that was not up to individuals to decide whether or not to take. This concern was particularly strong in the early phases of data protection, where tackling the social risks stemming from the mass-employment of information

[1251] This patchwork effect may also result from the existence of multiple intermediaries, each possibly following its own line of action.
[1252] Mantelero, 'La Gestione Del Rischio' (n 422) 484–485.

technologies was a priority in the policymakers' agenda [1253]. These risks were addressed mainly through the introduction of "prior checking" requirements that charged supervisory authorities with the task of reviewing and assessing intended processing operations, before their implementation[1254]. As already discussed, these *ex-ante* revision duties of DPAs were increasingly shrunken, mostly to leave room to enhanced *ex-post* monitoring tasks, coupled with the concurrent gradual allocation of risk assessment responsibilities on controllers and greater margins of appreciation for individuals[1255]. Under the DPD, *ex-ante* case-by-case assessments (i.e., "Prior Checking") were required only for a limited set of cases where, due to the presumed high-risk «to the rights and freedoms of data subjects» (whose identification was left to national discretion), DPAs were required to examine and authorize the concerned processing activities prior to their start[1256]. At the same time, the DPD required member states to impose on controllers the obligation to adopt «appropriate technical and organizational measures to protect personal data» against certain security risks[1257]. The provision ended up translating under many national laws as a standard checklist of "minimum-security measures"[1258], that controllers generally implemented as such,

[1253] Mayer-Schönberger (n 67) 223 ff; Bygrave (n 14) 93 ff; van der Sloot (n 621) 324; Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics' (n 624).
[1254]Bygrave (n 14) 70–77. Extensively under Chapter I, par. 3.
[1255] See also this Chapter, under par. 2.1 describing the role of DPAs.
[1256] As highlighted in Chapter I, the DPD included also a generalized "notification obligation" under Art. 18 before carrying out «any wholly or partly automatic processing operation», that was left widely unapplied at national level. Art. 20 DPD, instead, provided for the introduction of "Prior Checking" obligations that was further implemented under national laws. For example, Art. 17 of the 2003 Italian Privacy Code (legislative decree 2003/1996) introduced at national level a prior-checking obligation that required data controllers to notify to the Italian DPA processing activities that could entail «risks to the rights and freedoms of data subjects» and tasked the DPA to decide on their legitimacy. Stefano Bernardi, 'Commento All'art. 17: Trattamento Che Presenta Rischi Specifici' in C Massimo Bianca and Francesco Donato Busnelli (eds), *La protezione dei dati personali: commentario al D. lgs. 30 giugno 2003, n. 196: codice della privacy* (CEDAM 2007) 450. To determine for which data processing was required a prior notification, the Italian DPA drafted specific national guidelines (see e.g., the different provisions on biometric systems, video-surveillance, mobile remote payments).
[1257] See in particular recital 46 and Art. 17(1) of the DPD dedicated to "Security measures", that listed a series of possible risks primarily connected to security concerns: «Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data *against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access,* in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing».
[1258] In Italy, the provision was implemented first in Art. 15 of law 675/1996, then replaced by Articles 31-36 of the 2003 Italian Privacy Code, and "Annex B" which included a list of technical measures that controllers and processors were required to implement. See Vincenzo Caridi, 'Sub Art. 15' in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), *La tutela dei dati personali: commentario alla L. 675-1996* (2. ed, CEDAM 1999) 153 ff. and ; Salvatore Sica, Pasquale Stanzione and Giovanni Maria Riccio, 'Sub Art. 33', *La nuova disciplina della privacy: commento al D. lgs. 30 giugno 2003, n. 196* (Zanichelli 2005) 132 ff. Originally, the requirements under Annex B included also the draft of a "Security Planning Document" on a yearly basis, which involved a continuous risk assessment to

regardless of any more specific assessment that took into consideration the specific circumstances of the case[1259].

The overall approach to risk management under the DPD appeared to be quite limited. The concept of risk was narrowly construed; safeguard measures were mostly pre-established; and *ex-ante* assessments on an individual basis were reduced to a selected number of cases. The datafication of the society and the pervasive adoption of data-hungry technologies increasingly exacerbated the weaknesses of this model. Static security requirements could not contain the spiralling complexity and broadening of the types of risks stemming from new forms of personal data exploitation and DPAs were not able to cope with the exponential growth of processing activities[1260].

4.2 The novel approach under the GDPR: risk-based approach and accountability

With a view to modernize its vision and attitude towards data processing related risks, the GDPR expressly adopts and institutionalizes a "risk-based-approach"[1261] that introduces important changes in the risk management of processing activities.

The new regulation is explicit in embracing an extensive notion of risk that, as proved by the multiple references in the GDPR text[1262], should be broadly interpreted as including all the risks that data processing may produce to the "rights and freedoms of natural persons". The expression, as clarified by the WP29, is intentionally generic to concern primarily the right to privacy and data protection, but also other fundamental rights such

---

monitor the state of implementation of the security measures compared to the envisaged privacy risks. The obligation was however repealed in 2012, within the context of a simplification intervention (legislative decree 5/2012).

[1259] Even though a general obligation to implement all adequate and preventive security measures necessary was present, the standard practice was to apply by default the minimum-security measures already indicated by law, with no additional effort. Mantelero, 'La Gestione Del Rischio' (n 422) 476.

[1260] Raffaele Torino, 'La valutazione d'impatto (Data Protection Impact Assessment)' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), *La nuova disciplina europea della 'privacy'* (Wolters Kluwer 2016) 858. See also recital 89 GDPR that criticized the effectiveness of the general notification obligation included under the Directive, stating that «while that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data».

[1261] Giorgio Giannone Codiglione, 'Risk-based approach e trattamento dei dati personali' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), *La nuova disciplina europea della 'privacy'* (Wolters Kluwer 2016) 53 ff. See also Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (30 May 2014) WP218. The WP29 specified that the "risk-based approach" was not a new concept and could indeed be already found under the DPD, however with the GDPR the centrality and detail that the concept acquires are unprecedented.

[1262] See in particular recitals 74,75, 76, 77, 81, 85, 86, 9; Articles 27, 30, 33, 34, 35, 36 GDPR.

as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[1263].

In addition, according to the principle of accountability embodied by the GDPR, controllers are primarily responsible to ensure, and demonstrate, that the impacts of their intended processing activities have been adequately addressed[1264]. As a consequence, contrary to the previous framework, the GDPR does not provide controllers with a list of specific safeguards or security measures to implement, rather it requires them to carry out a prior evaluation of the risks that data processing may entail, taking into account «the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons»[1265], and subsequently adopt the measures they consider most appropriate to eliminate or mitigate them. By laying down a general obligation to assess and mitigate the envisaged risks, the provision represents the first layer of a "scalable" risk assessment[1266], whose requirements intensifies the more the risks entailed by the processing activity become severe. It also shows the intention to decentralize the *ex-ante* risk assessments, placing the burden on controllers rather than keeping it centralized under the supervision of DPAs[1267].

On top of the mentioned general obligation, the second layer of the "scalable" approach mentioned above is triggered when processing operations «are likely to result in a *high-risk* to the rights and freedoms of natural persons»[1268]. In this case, the GDPR requires controllers to carry out a DPIA, namely a formalized assessment process that needs to meet certain conditions, described under the GDPR.

4.2.1 Data Protection Impact Assessment (DPIA)

The DPIA is a particular version of the more general instrument of "Impact Assessment" (IA), a structured process for identifying the effects of a given activity, evaluating the

[1263] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (n 1261) 4.
[1264] Finocchiaro, 'Il Quadro d'insieme Sul Regolamento Europeo Sulla Protezione Dei Dati Personali' (n 420) 17 ff.
[1265] Art. 32 GDPR, named "Security of processing" which despite maintaining the reference to specific security risks, such as accidental or unlawful destruction, loss or alteration (par. 2), includes the risks to the "rights and freedoms" as an opening statement of the article (par. 1).
[1266] Article 29 Data Protection Working Party, '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' (n 427); Alessandro Mantelero, 'Valutazione d'impatto sulla protezione dei dati' in Roberto D'Orazio and others (eds), *Codice della privacy e data protection* (Giuffrè Francis Lefebvre 2021) 538.
[1267] Torino (n 1260) 857.
[1268] Art. 35 GDPR and recitals 90-91 GDPR.

impacts, thus potential harms/risks, it might cause, and allocating responsibilities for those impacts[1269]. It is as an effective mechanism to anticipate negative consequences and establish accountability for their mitigation or elimination. IAs have been a well-established practice in different domains, helping to investigate environmental, social, political and technological impacts[1270]. Starting from the mid-1990s, the concept of "Privacy Impact Assessment" (PIA) started also to emerge as an evaluation instrument for the potential impacts on individual privacy of systems or projects[1271]. Developments in PIA philosophy and methodology were largely developed in countries outside Europe (Australia, New Zeland and Canada)[1272]. Around the mid 2000s, signs of interests for an organized and wide-ranging impact assessment in the data protection context started to sporadically appear at EU level, driven mostly by the Anglophone experiences of UK[1273] and Ireland[1274], followed by a mild initial endorsement of the EU Commission[1275]. It was however only with the GDPR that the process of impact assessment (or according to GDPR terminology "D" PIA) was formally institutionalized[1276].

[1269] International Association for Impact Assessment, 'What Is Impact Assessment?' (International Association for Impact Assessment 2009) <https://www.iaia.org/reference-and-guidance-documents.php>.

[1270] ibid.

[1271] Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer Law & Security Review 123. According to Clarke, primary intellectual threads in the emergence of the concept of "PIA" were the idea of "Technology Assessment" and the "Environmental Impact Statements", both practiced in the US since the '70s, although the term "PIA" was used consistently only years later.

[1272] On the evolution of PIAs around the world, see David Wright and Paul de Hert (eds), *Privacy Impact Assessment* (Springer 2012) in particular chapters 5-10. Also, David Flaherty, 'Privacy Impact Assessments: An Essential Tool for Data Protection' (2000) 7 Privacy Law and Policy Reporter 85. According to Flaherty, the idea of using PIAs in a systematic manner to address data protection problems was pioneered by New Zealand, Australia and Canada since the mid-1990s.

[1273] In 2007, the Information Commissioner's Office (ICO) commissioned a team of experts to deliver a comprehensive review of PIAs laws and practices around the world, that was followed in December of the same year by a PIA Handbook, further revised in June 2009. Clarke (n 1271) 129; David Wright, Rachel Finn and Rowena Rodrigues, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries' (2013) 9 Journal of Contemporary European Research 160, 170–171.

[1274] In 2010, the Irish Health Information and Quality Authority (HIQA) produced a PIA Guidance, following its review of PIA practice in other jurisdictions, which became best practice in relation to PIAs. Wright, Finn and Rodrigues (n 1273) 168.

[1275] The EU Commission issued a Recommendation in May 2009 in which it encouraged the development of a «framework for privacy and data protection impact assessments" that should be submitted for endorsement to the Article 29 Data Protection Working Party». European Commission, 'Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification (Notified under Document Number C(2009) 3200)' (2009) 2009/387/EC. The EC also co-funded different projects (e.g., the "Privacy Impact Assessment Framework project", carried out by a consortium of Vrije Universiteit Brussel, Trilateral Research & Consulting and Privacy International) on existing PIA methodologies in other countries. Wright, Finn and Rodrigues (n 1273) 161.

[1276] The DPIA represents a "newer" version of PIA, that essentially reflects the best practices of the different PIAs methodologies developed around the world. Charles D Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 105404, 8; David

The imposition of a structured and documented procedure is directed at ensuring that in cases where the risk threshold is supposed to be elevated, controllers are able to demonstrate that they have carried out an exhaustive analysis of the possible risks of the data use and have taken appropriate safeguards to avoid the materialization of any detected harm.

(i) HIGH-RISK - Flexibility and adaptability are characteristic of this new approach. The element that triggers a mandatory DPIA is the presence of a *high risk*, whose existence needs to be determined by the controller. The GDPR provides a (non-exhaustive) list of general factors that may presumptively indicate when a processing operation should be considered high risk, including: (i) the use of new technologies[1277]; (ii) the systematic and extensive evaluation of personal aspects relating to natural persons (including profiling) used in the context of a decision-making process[1278]; (ii) large-scale processing of special categories of data or data related to convictions[1279]; (iii) systematic monitoring of publicly accessible areas[1280]. Further interpretative guidance has been offered by the WP29[1281] and national DPAs[1282] to help controllers assess the

Wright, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307; Mantelero, 'La Gestione Del Rischio' (n 422) 476.

[1277] Art. 35(1) GDPR. The general formulation employed by the GDPR, however, should not be read in the sense that whenever a "new technology" is used a DPIA is *per se* required, rather as a possible factor that may elevate the risk, thus triggering the DPIA requirement. Torino (n 1260) 861; Mantelero, 'Valutazione d'impatto sulla protezione dei dati' (n 1266) 547.

[1278] Art. 35(3)(a) GDPR. The norm does not require the processing to be "solely" automated, which means that the article covers both solely automated decision-making processes (as per Art. 22(1) GDPR) but and not wholly automated ones, when the human factor maintains a decisive role. Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478) 29; Mantelero, 'Valutazione d'impatto sulla protezione dei dati' (n 1266) 543.

[1279] Art. 35(3)(b) GDPR. Recital 91 offers some further guidance to clarify the concept of "large scale" stating that it concerns operations that «process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects». For a more practical, albeit limited, example, the article adds that «the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer». The concept remains context-based and needs to be assessed on the basis of the elements of the concrete situation.

[1280] Art. 35(3)(c) GDPR. According to the WP29 the risk for this type of monitoring may be high because personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used, and it may be impossible for individuals to avoid being subject to such processing in public. Article 29 Data Protection Working Party, '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' (n 427) 9.

[1281] In particular, the already mentioned Article 29 Data Protection Working Party, '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' (n 427). The Guidelines identify nine criteria that adds up and expand those already provided under the GDPR to identify a possible "high risk", including: (i) matching or combining data sets; (ii) data relating to vulnerable data subjects; (iii) innovative use or application of new technological or organizational solutions.

risk threshold of their intended processing activities and determine whether a DPIA is necessary. They have also provided user-friendly tools to facilitate the conduction of these assessments[1283].

(ii) ASSESSMENT PROCEDURE - Flexibility is central also with reference to the practical assessment procedure. The GDPR does not impose a fixed methodology and allow data controllers to establish the structure, form and way in which the DPIA is carried out, drawing from existing working practices and sector peculiarities[1284]. Art. 35 (7) GDPR lists only the main contents that each DPIA needs to include, which essentially reproduce the phases in which the assessment process should develop[1285]. These include: (i) a description of the process/product/activity; (ii) the evaluation of the necessity and proportionality of the processing; (iii) the investigation of the risks for the rights and freedoms of persons, based on the *context* of the processing (nature, scope, purposes); the *type* of risks (i.e., interests impacted) and its *sources*; the *severity* and *likelihood* of the risk[1286]; and finally (iii) the definition of measures envisaged to address the risks[1287]. Also, the DPIA is not intended to be a one-time exercise, rather a "continuous process" that involves periodic re-assessments and revision throughout the lifecycle of the processing activity to keep the risk information up to date and evaluate the effectiveness of the mitigating measures[1288].

(iii) STAKEHOLDERS - The main stakeholder of the entire process remains the data controller. Data subjects may in theory be engaged and express their views during the

---

[1282] See e.g. the list of processing activities that require/do not require a DPIA published by national DPAs, including the Italian DPA: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979; the French CNIL: https://www.cnil.fr/fr/liste-traitements-aipd-non-requise ; and the Spanish AEPD: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluciones-impacto.

[1283] For example, the software developed by the CNIL (available in 20 languages) to help controllers carry out the DPIA, available at: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

[1284] Despite different tools and methodologies have been promoted to facilitate the performance of DPIAs, there is no fixed DPIA methodology. On the contrary, the WP29 encourages the development of sector-specific DPIA frameworks to draw on specific sectorial knowledge and tailor the assessment to the specific features and needs of the sector (e.g., particular types of data, corporate assets, potential impacts, threats, measures). Article 29 Data Protection Working Party, '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' (n 427) 17.

[1285] Mantelero, 'La Gestione Del Rischio' (n 422) 500.

[1286] Recital 90, Torino (n 1260) 868 ff.

[1287] Art. 35(7)(d) GDPR. The safeguards should include «safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned».

[1288] Article 29 Data Protection Working Party, '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' (n 427) 14.

procedure[1289], however the provision has been implemented very poorly and, in the majority (if not all) cases, their contribution is not taken into account. Other forms of external advice from independent experts, instead, are simply recommended[1290], but not required. DPAs are the only actors that keep certain supervisory tasks on the overall assessment procedure, albeit in a very narrow set of circumstances. Evolving the "prior checking" rule of the DPD, the GDPR provides that whenever the "residual" risks after the DPIA has been carried out are still high, hence the controller has not been able to find sufficient measures to reduce the risks to an acceptable level, the supervisory authority needs to be consulted[1291]. The authority shall review the envisaged processing and determine whether the processing infringes the GDPR, agreeing in the case with the DPA on additional mitigating measures to implement. Whether to involve or not the authority, however, remains a choice that depends on the controller internal self-assessment.

In essence, the DPIA model embraces an *ex-ante* approach to risk assessment and an (hypothetical) broad understanding of concerned risks, thus ideally preventing dangerous and harmful processing activities to be set in motion. It allocates the main assessment and mitigating functions to data controllers, thus relieving data subjects from the need to evaluate these risks themselves and avoiding to overload the desks of supervisory authorities, at the same time keeping the latter in the loop to review the most threatening scenarios. It imposes documentation requirements, thus ensuring that compliance can be subsequently proved and monitored. In light of this, the DPIA procedure appears to have, on paper, all the ingredients to address the risks of data uses in a wide-ranging, but also realistic manner.

ISSUES - In practice, however, the DPIA model has visibly failed to prevent the implementation of data practices that are clearly harmful for individuals, for their discriminatory, manipulative or intrusive effects. DPIAs are often treated as managerial

[1289] Art. 35(9) GDPR does include the faculty for controllers to «seek the views of data subjects or their representatives», however the provision has never been given much emphasis. While in the original proposal of the Commission, consultation with data subjects was included as a mandatory requirement, because it was deemed to be an excessively heavy burden for controllers, it was later softened adding the wording "where appropriate" to the norm. Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22, 28.

[1290] The WP29 considers "good practice" to seek advice from independent experts of different professions (lawyers, IT experts, security experts, sociologists, ethics, etc.). Article 29 Data Protection Working Party, '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' (n 427) 15.

[1291] Art. 36 GDPR, that regulates the prior checking procedure, now under the name of "Prior Consultation".

exercises approached with a "box-ticking" method rather than a reflective, deeper understanding upon which real changes could be generated[1292]. Despite the language efforts in the GDPR, risks remain very much oriented on data quality and security, rather than a more in-depth assessment over the fundamental rights of individuals[1293]. The large margin of judgment that is left to controllers in assessing and managing data protection risks does also raise doubts on whether they are best placed to do the job, with so little external oversight in place[1294].

The DPIA procedure is not the only IA methodology developed as a response to the growing concerns on the use of data and data-intensive applications. Other variations of IA have been advanced in the context of emerging technologies as a way to tackle growing individual and societal risks. These alternative models may provide some useful lessons to be learnt for complementing, improving and evolving the current DPIA process into something more effective, albeit equally pragmatic.

4.2.2 Variations Of "Impact Assessments": ETiA, HRIA and AIA

The precursor and inspiration for the varying impact assessment models that have developed during time has been identified in the Environmental Impact Statement (EIS), established in 1969 under the US National Environmental Policy Act (NEPA)[1295], that required US federal agencies that intended to perform actions significantly affecting the "human environment" to perform an assessment of their impacts[1296]. Since then, the EIS has been used, adapted, evolved by different commentators as a regulatory model for impact assessment in other contexts[1297]. This section focuses in particular on three alternative IAs that, beside the already mentioned PIA and DPIA, have been employed in the field of data protection and emerging technologies: Ethical Impact Assessment

[1292] Raab (n 345) 8.
[1293] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754, 761.
[1294] Maria Eduarda Gonçalves, 'The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective' (2020) 23 Journal of Risk Research 139, 5–6.
[1295] US National Environmental Policy Act of 1969, Pub.L. 91–190, approved January 1, 1970. 42 U.S.C. § 4321 *et seq.*
[1296] See A Michael Froomkin, 'Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements' (2015) 2015 University of Illinois Law Review 1713, 1749; Clarke (n 1271) 125.
[1297] Froomkin, for example, uses EIS as a regulatory model in the privacy context, on which he bases his proposed "Privacy Impact Notice". Froomkin (n 1296) 1751 ff. Some of the assessment models analysed below also trace their origins to the EIS, for example Mantelero's HRESIA, Mantelero, 'AI and Big Data' (n 1293) 757–758. and Selbst's AIA, Andrew D Selbst, 'Disparate Impact in Big Data Policing' (2017) 52 Georgia Law Review 109, 169.

(ETiA) [1298]; Human Rights Impact Assessment (HRIA) and the Algorithmic Impact Assessment (AIA), taking into account also their internal variations. The analysis highlights the different approaches and techniques employed in these assessments, to draw useful elements for a comparison with those currently adopted under the DPIA model.

A. *ETHICAL IMPACT ASSESSMENT (ETiA)* – Even though ethics assessment is a well-established practice particularly in the medical research field, there has been a growing institutionalization of this type of assessment in non-medical fields[1299]. The ethical challenges raised by emerging technologies have led to the development of an ETiA, a particular approach within the realm of ethics assessment that expands impact assessment to the realm of ethics and aims at anticipating and ethically appraising the utilisation of technology in society before such utilisation takes place[1300].

According to Wright, an ETiA can be defined a «process during which an organization, together with stakeholders, considers the ethical issues or impacts posed by a new project, technology, service, program, legislation, or other initiative, to identify risks and solutions»[1301]. Similar to PIAs and DPIAs, this type of exercise represents a way «to avoid any nasty fallout from consumers or policy-makers who might feel that the technology as implemented works to the detriment of generally accepted social values»[1302] and adopt the necessary mitigating measures.

ETiA has a number of peculiarities compared to other forms of IA. First, ETiA is concerned with impacts that have *ethical relevance* or that raise *ethical issues*, which encompass a broader set of values than those traditionally considered, for example, in standard DPIAs. These include impacts that look more broadly at the benefits and harms, justice and fairness, well-being and social good[1303] of new

[1298] Although this type of assessment is commonly referred to as "ETA" (e.g., David Wright, 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13 Ethics and Information Technology 199.) to avoid confusion with the cousin Environmental Impact Assessment, Mantelero refers to it as ETiA, Mantelero, 'AI and Big Data' (n 1293) note 25.

[1299] SATORI Project, 'Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and Selected Other Countries' (SATORI Project 2016) Deliverable D1.1 54–55 <https://satoriproject.eu/work_packages/comparative-analysis-of-ethics-assessment-practices/>.

[1300] ibid 47. See further, Annex 2 (2.b -Engineering Science) of this report.

[1301] Rowena Rodrigues, 'David Wright, Trilateral Ltd. - Ethical Impact Assessment Will Make R&I More Responsible!' <https://satoriproject.eu/publications/trilateral-david-wright/> accessed 16 November 2021.

[1302] Wright (n 1298) 223.

[1303] SATORI Project (n 1299) 30.

technologies. Because ethical principles and values are highly context-dependent, the value frame of reference to conduct an ETiA needs to be identified by the assessor on a case-by-case basis. Some of the proposed methodologies for an ETiA framework provide some guidance in this respect. In his proposal, for example, Wright borrows the ethical values from healthcare decision making[1304] (respect for autonomy, non-maleficence (no harm), beneficence and justice), and he further adds the principles of privacy and data protection to the ethical value catalogue[1305]. Even though different methodologies may adopt different value frames, they mainly refer to rights and freedoms set forth in the main EU and international Charters, and to broader social and collective interests including social justice, equality, and the well-being of the collectivity[1306]. These values/issues are generally accompanied by a set of questions to facilitate ethical considerations and help assessors identify in practice the ethical impacts of the technology[1307]. The assessment is supported also by a list of ethical tools and procedures (e.g., expert consultations, surveys, expert workshops, checklists of questions) that should help the assessor gather insights about how the technology is perceived and to determine the measures that would make the technology ethically acceptable[1308].

Participation and *consultation with stakeholders* (i.e., a group or an individual who is affected by or has an interest in the assessed project) are also fundamental aspects of an ETiA, as they enable these parties to voice their concerns and interests as part of the process, helping to anticipate utilisations and possible impacts[1309]. Stakeholders' engagement can be achieved through different mechanisms, although it may vary depending on the scale of assessment (the larger the assessment, the more the participatory effort). Finally, ETiA is characterized by the requirement of *publication* or public presentation of the final assessment, including the evaluation of the ethical issues and the remedial actions adopted accordingly[1310], and the

[1304] He borrows in particular the four principles posited by Beauchamp and Childress in their work on biomedical ethics. Tom L Beauchamp and James F Childress, *Principles of Biomedical Ethics* (5th ed, Oxford University Press 2001).
[1305] Wright (n 1298) 204.
[1306] See different methodologies described in SATORI Project, 'A Common Framework for Ethical Impact Assessment - Annex 1' (SATORI Project 2016) Deliverable D4.1 59 ff. <https://satoriproject.eu/work_packages/roadmap-for-a-common-eu-ethics-assessment-framework/>.
[1307] E.g., Wright (n 220) 204 ff.; SATORI Project (n 228) 20 ff.
[1308] Wright (n 1298) 215.
[1309] SATORI Project (n 1306) 31 ff.; Wright (n 1298) 218.
[1310] SATORI Project (n 1306) 37.

existence of a procedure of *third-party review and audit* of the final assessment[1311]. Both requirements increase the transparency of the process and enhance the accountability towards the implementation of the indicated mitigating measures.

The similarity between the ETiA and PIA processes and the complementarity of their contents led Wachter and Friedman to support the adoption of an integrated assessment, that amalgamates the ETiA approach with PIA elements[1312]. The result is a comprehensive systematic "P+ETiA" model for the assessment of the implications of emerging technologies. Other initiatives have emerged in recent years to support the development of a systematic approach to the assessment of privacy and ethical implications stemming from new systems, applications and technologies (see e.g., EPIA+[1313]; PESIA framework[1314]). Publicity of the assessment and mandatory participation are key aspects.

Variations to the standard ETiA model have also been proposed. Some of them, contrary to the technology-neutral approach of the ETiA, target specific technological challenges. Raab and Wright, for example, advocates the implementation of a "Surveillance Impact Assessment" (SurvIA) that is designed as an anticipatory response to surveillance practices[1315]. The SurvIA model is tailored to address the ethical issues raised in the surveillance context, both in scope (surveillance technologies[1316]) and underlying value frame (that includes privacy related issues, as well as other ethical, social, economic and political interests of individuals and groups[1317]). Many are the similarities between SurvIA and ETiA. In particular, both are more societally oriented than D(PIA)s, and are more explicit in recognizing the broader ethical and social risks of new technologies and systems. Both place great emphasis on the engagement of relevant stakeholders, on the importance of

[1311] Wright (n 1298) 221.
[1312] David Wright and Michael Friedewald, 'Integrating Privacy and Ethical Impact Assessments' (2013) 40 Science and Public Policy 755.
[1313] 'The Importance of the Ethical and Privacy Impact Assessment Plus in the INGENIOUS Project' (*Trilateral Research*, 7 December 2020) <https://www.trilateralresearch.com/the-importance-of-the-ethical-and-privacy-impact-assessment-plus-in-the-ingenious-project/> accessed 16 November 2021.
[1314] 'What's the PESIA Framework? – VIRT-EU' (*virt.eu*, 30 October 2018) <https://blogit.itu.dk/virteuproject/2018/10/30/whats-the-pesia-framework/> accessed 16 November 2021.
[1315] Charles Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul de Hert (eds), *Privacy impact assessment* (Springer 2012) see also, David Wright and Charles D Raab, 'Constructing a Surveillance Impact Assessment' (2012) 28 Computer Law & Security Review 613.
[1316] Understood as a broad set of «technology-assisted processes for watching, listening, physical inspection, tracking, sensing, 'dataveillance', and the like, whether overtly or through covert means, and whether in 'real' space or cyberspace». Raab (n 1276) 9.
[1317] Raab and Wright (n 1315) 376–382.

transparency and publicity of the assessment process and on a third-party independent review of the assessment results[1318].

ETiA has not received substantial policy attention in the regulation of new technologies. However, there have been occasional references to ethically-oriented risk assessments in institutional documents concerning processing of personal data. The "Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data" (hereinafter "Guidelines")[1319], adopted in 2017 by the Council of Europe embraces this vision. Within the broader purpose of the document to contextualize the principles of data protection in the big data scenario, the instrument of risk assessment was attributed a prominent role. In this light, the CoE expressly addresses the need to adopt an approach that does no longer primarily focus on "individual control" and data quality/security issues, rather considers different kinds of implications concerning data uses[1320]. After acknowledging that «the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights»[1321], the Guidelines stress the importance for controllers to «adequately take into account the likely impact of the intended Big Data processing and its broader ethical and social implications to safeguard human right and fundamental freedoms»[1322]. Despite the high-level nature of the Guidelines, the CoE provides a few practical indications. In particular, it states that the common guiding and ethical values against which conducting the assessment should be retrieved from international charters of human rights and fundamental freedoms, such as the European Convention on Human Right. In addition, aware of the difficulties that controllers may face in conducting such a comprehensive assessment, the Guidelines propose the employment of "*ad*

[1318] Wright and Raab (n 1315); Raab (n 1276) 10.
[1319] Council of Europe, 'Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data' (2017) T-PD(2017)01.
[1320] Alessandro Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law & Security Review 584, 591. The author points out that the Guidelines «do not consider the notion of control as circumscribed by individual control (i.e. notice and consent), but adopt a broader idea of control over the use of data, according to which, individual control "evolves in a more complex process of multiple-impact assessment of the risks related to the use of data».
[1321] Council of Europe (n 1319) par. 2.3. The Guidelines also state that «since Big Data makes it possible to collect and analyse large amounts of data to identify attitude patterns and predict behaviours of groups and communities, the collective dimension of the risks related to the use of data is also to be considered» (Introduction).
[1322] ibid par. 1.1.

hoc ethical committees"[1323]. These committees of experts should help controller to identify the specific ethical values to be safeguarded with regard to a given use of data, providing more detailed and context-based guidance for risk assessment[1324].

B. *HUMAN RIGHTS IMPACT ASSESSMENT* – A Human Rights Impact Assessment ("HRIA") can be defined as a «process for identifying, understanding, assessing and addressing the adverse effects of a business project or activities on the human rights enjoyment of impacted rights-holders such as workers and community members»[1325]. The HRIA methodology has gained traction in different fields[1326], particularly in the business sector due to the emphasis placed in the last decade on the accountability of businesses in the exercise of human rights due diligence[1327]. The Danish Institute for Human Rights has provided a comprehensive guide and toolkit on the conduction of HRIA in the context of business projects and activities. Briefly put, the HRIA process is traditionally very lengthy and complex, as it is typically undertaken on large-scale impacting projects (e.g., mine sites, oil and gas plants), however its key elements remain the same even when applied, in a scaled down form, to smaller business projects[1328]. Contrary to ETiAs, where the basis for the assessment is formed by a heterogeneous range of social values and principles, in the HRIA the benchmark for the assessment is formed by *internationally recognized human rights* standards and principles[1329]. *Meaningful participation* of rights-holders, companies (duty-bearers) and other human rights stakeholders are core aspects of this impact assessment process. Particular attention is placed on the inclusiveness and representativeness of the stakeholders' engagement process; the level of information sharing involved in participation and consultation activities; the empowerment and capacity building of individuals to participate in the impact

[1323] ibid par. 1.3; Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (n 1320) 593–595.
[1324] Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (n 1320) 594.
[1325] Nora Götzmann and others, 'Huma Rights Impact Assessment - Guidance and Toolbox' (The Danish Institute for Human Rights 2016) 10.
[1326] See e.g., James Harrison and Mary-Ann Stephenson, 'Human Rights Impact Assessment : Review of Practice & Guidance for Future Assessments.' (Scottish Human Rights Commission 2010).
[1327] Particularly after the endorsement by the Human Rights Council, in 2011, of the UN Guiding Principles on Business and Human Rights, that establish that businesses have a responsibility to respect human rights, using a process of "due diligence" that includes identifying, avoiding, mitigating and remediating the human rights impacts with which they are involved.
[1328] Götzmann and others (n 397) 8.
[1329] Götzmann and others (n 1325) 33 ff.

assessment process[1330]. Finally, *accountability* of duty-bearers, *transparency* of the assessment process - including public communication of the impact assessment findings – and mechanisms to ensure the implementation of *mitigating measures* are all characteristic features of the HRIA framework[1331].

Even though traditionally HRIA is employed in the business context, the challenges that digital technologies are raising to human rights have prompted to re-evaluate the HRIA methodology and tailor the assessment process to AI applications and algorithmic processes[1332]. Along these lines, Mantelero has proposed two different variations of HRIA, adapted to the issues raised by emerging technologies. The first model is defined Human Rights, Ethical and Social Impact Assessment ("HRESIA"), which, in the author's view, «may contribute to the evolution of the existing DPIA towards a more complete assessment model […] that put into practice the EU legislator's intention to safeguard not only the right to the personal data protection, but also the "fundamental rights and freedoms of natural persons"»[1333]. HRESIA takes up the human rights-focus of HRIA and complements it with attention to societal and ethical consequences of data use (closer to the ETiA approach)[1334]. More specifically, ethical and social values are used as "interpretative filters" of human rights, to overcome their individualistic dimension and give adequate consideration to collective and group issues concerning modern data uses, but also to contextualize the application of human rights taking into account regional and local differences. The model architecture is made up of a *questionnaire*, that serves as a self-assessment tool to guide data controllers[1335] and facilitate the identification of the relevant human rights issues for any given application[1336]. In addition, drawing inspiration from the CoE Guidelines, the author supports the employment of *ad hoc* expert committees (HRESIA committees)[1337], equipped with the proper skillset to

[1330] ibid 94 ff.
[1331] ibid 75 ff.
[1332] Mark Latonero, 'Governing Artificial Intelligence' (*Data & Society*, 10 October 2018) <https://datasociety.net/library/governing-artificial-intelligence/> accessed 17 November 2021.
[1333] Mantelero, 'AI and Big Data' (n 1293) 768.
[1334] ibid 766–767.
[1335] Compared to other models, Mantelero uses specifically the terminology employed in the data protection context, therefore identifying the assessor in the "data controller". Other IA models use a more generic language, having a general application in the field of "emerging technologies" rather than a specific focus on "data protection".
[1336] Mantelero, 'AI and Big Data' (n 1293) 769.
[1337] See Council of Europe (n 1319) par. 1.3; Mantelero, 'AI and Big Data' (n 1293) 770–771.

support controllers in the correct evaluation and mitigation of the envisaged risks [1338]. The prosed HRESIA remains, as of today, a theoretical blueprint that provides an outline of the overall model but does not offer deeper insights on each of its elements.

A more comprehensive methodology has been advanced by the same author with an enhanced HRIA model contextualized to the issues raised by AI data-intensive systems[1339]. Compared to HRESIA, the new "AI-HRIA" downsizes the role of ethics to prioritize human rights and abandons the technology-neutral approach to focus on a specific technological development (AI based applications)[1340]. The proposed "operational approach" to human rights assessment in AI offers a list of rights and freedoms potentially impacted by data intensive systems, extracted from an evidence-based analysis of DPAs' jurisprudence, and a detailed description of the main building blocks and procedural steps which constitute the model[1341]. An additional layer, compared to other proposed methodologies, is the hypothetical test of the proposed AI-HRIA on two existing use cases: a small scale one (the "Hello Barbie" product)[1342] and a large-scale multi-factor one (the Canadian smart-city project "Sidewalk")[1343]. Mantelero's framework is very similar to the "HRIA model of Digital Activities" developed by the Danish Institute for Human Rights on the benchmark of the previous "business HRIA" guidance and better tailored to the digital ecosystem[1344]. Without deep-diving into the details of the model, what emerges from an overview of both digital-oriented HRIAs is that their recurring traits essentially mirror the characteristic features of the traditional HRIA, in particular: heavy stress on *stakeholders' engagement*, the *transparency* of the process results and implementing mitigating measures.

The application of HRIAs in relation to digital activities and data-driven technologies is still in its infancy. However, a few examples of HRIA related to digital services and products have already hit the news. Since 2018, following the international uproar on

[1338] Mantelero, 'AI and Big Data' (n 1293) 771; Raab (n 1276) 12.
[1339] Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 105561.
[1340] On the debate on 'ethics' and 'human rights' see ibid 4 ff.
[1341] ibid 7–21.
[1342] ibid 21.
[1343] ibid 29.
[1344] Emil Lindblad Kernell, Cathrine Bloch Veiberg and Claire Jacquot, 'Guidance on Human Rights Impact Assessment of Digital Activities' (The Danish Institute for Human Rights 2020).

the role of the social network Facebook in the fuelling of violent conflicts around the world, the company partnered with external consultants to undertake HRIAs and assess the impacts resulting from the use of its social platform on individuals in Myanmar, Sri Lanka, Cambodia and Indonesia[1345]. An HRIA report was also released in 2019 by Google, which commissioned a third-party assessment on its facial recognition technology in the Media and Entertainment[1346].

C. *ALGORITHMIC IMPACT ASSESSMENT* – Researches, institutions and civil organizations have referred to Algorithmic Impact Assessments ("AIAs"), as a way to address the negative outcomes to individuals and the society at large of algorithmic systems[1347]. Despite its accepted use, the term AIA has no agreed definition and it currently encompasses an array of models that share as a common feature a focus on algorithmic processes. Unlike the other types of assessments described above, which are rooted in methodologies that were already established in certain non-technological fields and were further adjusted to the technological context, AIAs have not a clear ancestor and borrow their typical attributes from other domains (HRIA, DPIA, ETiA)[1348].

Existing initiatives and regulatory proposals on AIA have largely targeted algorithmic systems employed by public agencies in the context of public sector activities, where the request for transparency and public accountability is growing. Selbst was one of the first authors to outline the potential use of impact assessment methods for software procurement in government agencies[1349]. Focusing in particular on automated decision systems used in the criminal justice context, Selbst stressed the

---

[1345] 'An Update on Facebook's Human Rights Work in Asia and Around the World' (*Meta*, 12 May 2020) <https://about.fb.com/news/2020/05/human-rights-work-in-asia/> accessed 17 November 2021; 'Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections' (n 1156); Lindblad Kernell, Bloch Veiberg and Jacquot (n 1344) 24.

[1346] 'Google's Human Rights by Design' (*BSR*, 30 October 2019) <https://www.bsr.org/en/our-insights/blog-view/google-human-rights-impact-assessment-celebrity-recognition> accessed 17 November 2021.

[1347] Selbst (n 1297); Dillon Reisman and others, 'Algorithmic Impact Assessment: A Pracical Framework for Public Agency Accountability' (AI Now 2018); Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2021) 11 International Data Privacy Law 125; Michele Loi and others, 'Automated Decision-Making Systems in the Public Sector – An Impact Assessment Tool for Public Authorities' (Algorithmic Watch 2021). The necessity to assess the impacts of algorithms on individuals and collectivity has also been stressed at various institutional levels (see e.g., European Parliament. Directorate General for Parliamentary Research Services., *A Governance Framework for Algorithmic Accountability and Transparency.* (Publications Office 2019).

[1348] Kaminski and Malgieri (n 1347) 136; Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' (Data&Society 2021).

[1349] Selbst (n 1297).

benefits of a strong regulatory requirement for AIAs. An obligation to conduct an assessment would in fact publicly expose the potential criticalities of decision-making systems, which would not only favour algorithmic transparency but, coupled with public consultation mechanisms and judicial review, it would increase accountability of public agencies[1350]. Following these premises, some organizations (AI Now Institute[1351] and Algorithmic Watch[1352]) have developed practical AIA frameworks to support public authorities in the evaluation of the potential risks in the use of existing and proposed automated decision systems. All these models stress the importance for a series of requirements similar to those already analysed under ETiAs or HRIAs, which include (i) early disclosure of useful information about the interested process and continuous public engagement with affected stakeholders; (ii) third-party review processes (e.g., external researcher review or other type of audit procedures) and enhanced transparency (e.g., introduction of a public register for automated decision systems employed in the public sector). Kaminski and Malgieri envision a model of AIA[1353] inspired and possibly fitting within the GDPR framework, that builds on the experience and components of the DPIA, but accentuates certain key elements: engagement of impacted individuals; participation of external experts; disclosure duties and involvement of DPAs[1354].

While proposals from civil society and academia are abundant[1355], there have been some mild moves in this direction also at policy level. Outside the EU, both Canada and the US have made steps in this direction. With the adoption of the Directive on Automated Decision-Making[1356], the Canadian Treasury Board introduced AIA as a mandatory risk assessment tool for any government agency using such system or any vendor using such system to serve a government agency[1357]. According to the Board, this AIA is «designed to help departments and agencies better understand

[1350] ibid 173–178 see also ; Moss and others (n 1348) 29; Kaminski and Malgieri (n 1347) 136.
[1351] Reisman and others (n 1347).
[1352] Loi and others (n 1347).
[1353] Kaminski and Malgieri (n 1347).
[1354] ibid 139–140.
[1355] Along the models mentioned above, see also the ECP | Platform voor de InformatieSamenleving, 'Artificial Intelligence Impact Assessment' (ECP | Platform voor de InformatieSamenleving 2018) <https://ecp.nl/publicatie/artificial-intelligence-impact-assessment-english-version/> accessed 17 November 2021.
[1356] Treasury's Board Directive on Automated Decision-Making, taking effect on April 2019, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.
[1357] Section 6 of the Directive on Automated Decision-Making, "Algorithmic Impact Assessment".

and manage the risks associated with automated decision systems»[1358] and provide them appropriate governance, oversight and reporting/audit requirements[1359]. The AIA is structured to be an electronic survey[1360], where each answer is coded with five scoring categories that add or remove risk depending on the answer and will determine the final impact level. The questionnaire is expected to be reviewed on a regular basis. The US have also opened the discussion on AIA. In 2019, the Algorithmic Accountability Act[1361] was proposed to the Congress. The Act requires specific commercial entities to conduct assessments of high-risk systems that involve personal information or make automated decisions, such as systems that use artificial intelligence or machine learning[1362]. Although the bill has the merits of extending AIA beyond the public sector, the proposal, as it stands today, seems to lack incisiveness, partly due to the absence of mandatory publication of the assessment's results, drastically reducing the transparency and oversight thresholds[1363].

At EU level, one EU member state, Slovenia, made a fleeting attempt to include algorithmic impact assessment (AIA) as a specific and additional safeguard in the context of automated decision-making in one of the drafts of the Data Protection Act complementing some aspects of the GDPR at domestic level[1364]. The inclusion seems however to have been deleted from the latest draft[1365].

[1358] Treasury Board of Canada Secretariat, 'Algorithmic Impact Assessment Tool' (22 March 2021) <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> accessed 17 November 2021.

[1359] Supergovernance, 'A Canadian Algorithmic Impact Assessment' (*Medium*, 18 March 2018) <https://medium.com/@supergovernance/a-canadian-algorithmic-impact-assessment-128a2b2e7f85> accessed 17 November 2021; Supergovernance, 'The Government of Canada's Algorithmic Impact Assessment: Take Two' (*Medium*, 8 August 2018) <https://medium.com/@supergovernance/the-government-of-canadas-algorithmic-impact-assessment-take-two-8a22a87acf6f> accessed 17 November 2021.

[1360] The electronic survey is available at: https://open.canada.ca/aia-eia-js/?lang=en .

[1361] Yvette D. Clarke, "H.R.2231—116th Congress (2019–2020): Algorithmic Accountability Act of 2019,"2019, https://www.congress.gov/bill/116th-congress/house-bill/2231. The bill has never progressed past the committee level, although is expected to be updated and reintroduced for discussion Grace Dille, 'Sen. Wyden to Reintroduce AI Bias Bill in Coming Months' (19 February 2021) <https://www.meritalk.com/articles/sen-wyden-to-reintroduce-ai-bias-bill-in-coming-months/> accessed 17 November 2021. Meanwhile, other algorithmic-related federal bills have been introduced, like the "Algorithmic Justice and Online Platform Transparency Act of 2021" (https://www.congress.gov/bill/117th-congress/house-bill/3611/text) that proposes to prohibit the discriminatory use of personal information by online platforms in any algorithmic process, to require transparency in the use of algorithmic processes and content moderation, and for other purposes. The act includes also an "assessment" requirement to exclude the existence of any discriminatory outcome from the algorithmic process (section 4(a)(2)(A)(iv).

[1362] Algorithmic Accountability Act of 2019, section 3(b)(1).

[1363] Moss and others (n 1348) 33.

[1364] Malgieri (n 1033) 18. The author refers to Art. 42(5) of one of the first drafts of the Slovenian Data Protection Law implementing the GDPR (*Predlog Zakona o varstvu osebnih podatkov – predlog za*

More specific interventions from the EU have been pursued in the context of those sophisticated algorithmic decision systems that fall under the umbrella of "AI" systems, taking so far two parallel paths. As a result of the works of the High-Level Expert Group on Artificial Intelligence (AI HLEG), set up by the EU Commission in 2018 to provide support in the creation of the European Strategy for Artificial Intelligence, the "Ethics Guidelines for Trustworthy AI"[1366] were published. The Guidelines identified the core principles and requirements for trustworthy AI, along with an assessment list of questions that aimed to operationalize the requirements[1367]. The list, after further revisions, was finalized in a formal "Assessment List on Trustworthy AI" (ALTAI) that was rendered as an electronic portal[1368] to help organizations conduct self-evaluations of AI systems (developed, deployed, procured or used) and understand the possible underlying risks. This type of algorithmic (AI) assessment remains a supporting tool, whose employment occurs on an entirely voluntary basis. Further, in April 2021, the EU Commission released the first draft of AI Act[1369] that aims to establish an "ecosystem of trust" to guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU[1370]. One of the defining aspects of the new proposal is the adoption of a three-tier structure informed by a risk-based approach to AI systems. The top layer of this structure comprises prohibited AI systems, as they entail unacceptable risks[1371]; while the bottom includes limited risk

---

obravnavo – nujni postopek – Novo Gradivo ŠT. 2, http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp. gov.si/novice/2018/ZVOP-2 _ NG _ 2 _ apr.pdf.), that provided for a "specially focused assessment" prior to the introduction of a system of automated decision-making.

[1365] *Predlogom Zakona o varstvu osebnih podatkov (ZVOP-2)*, that appears to have removed par. 5 of Art. 42 available at: https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208.

[1366] High Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI.' (European Commission - Directorate General for Communications Networks, Content and Technology 2019).

[1367] ibid see in particular p. 24 ff.

[1368] The prototype web tool of the ALTAI is available at: https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence

[1369]European Commission, 'Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2021) COM(2021) 206 final.

[1370]See European Commission, 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust' (2020) COM(2020) 65 final; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Fostering a European Approach to Artificial Intelligence' (2021) COM(2021) 205 final.

[1371] Art. 5 of the AI Act.

AI systems, with specific transparency requirements, or minimal risk systems, subject only to voluntary codes of conducts[1372]. The middle layer, instead, includes a list of *high-risk AI systems* that in order to be deployed need to meet a range of technical and regulatory requirements, including undergo an *ex-ante* "conformity assessments"[1373]. Although the introduction in the AI context of this prior "conformity assessment" may suggest the adoption at EU level of a fully-fledge AIA, despite mandatory only for high-risk AI systems, from a closer look at the provision it becomes clear that this type of assessment has a much narrower scope. The wording ("*conformity*", which draws to the idea of complying with technical standards) and the contents (centered mostly on data quality and security) of the evaluation suggest a closer connection with product compliance rules than impact assessment ones. The emphasis is more on bureaucratic standardization, than on rights and values impacted by the system use. Equally, there is no requirement of publicity or third-party review and few opportunities for public consultation[1374]. For this reason, organizations have stressed the need to ensure that all high-risk AI systems are obliged to perform, on top of the conformity assessment, either a data protection impact assessment (DPIA), or a human rights impact assessment (HRIA)[1375]. In any case, being only the first draft of what is anticipated to be a long and debated adoption journey, the provisions of the current proposal are likely to be subject to multiple revisions.

4.3 Concluding remarks

The review of the different IA models available or developing in the field of emerging technologies helped to highlight different aspects that currently lack in the DPIA process

[1372] Art. 52 and Art. 69 of the AI Act.
[1373] Title III, Chapter 4-5 of the AI Act. The proposal distinguishes conformity assessment procedures to be followed based on the type of AI system assessed. In particular, (i) AI systems that are safety components of products follow third-party conformity assessment procedures (already established under the relevant sectoral product safety legislation), as well as real time remote biometric systems; (ii) other standalone high-risk AI systems follow a conformity assessment procedure based on "internal checks".
[1374] Moss and others (n 1348) 34.
[1375] Access Now, 'How to Fix the EU Artificial Intelligence Act' (*Access Now*, 7 September 2021) <https://www.accessnow.org/how-to-fix-eu-artificial-intelligence-act/> accessed 17 November 2021; AlgorithmWatch, 'AlgorithmWatch's Response to the European Commission's Proposed Regulation on Artificial Intelligence – A Major Step with Major Gaps' (*AlgorithmWatch*) <https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/> accessed 17 November 2021; European Digital Rights (EDRi), 'Open Letter: EDRi Urges Enforcement and Actions for the 2 Year Anniversary of the GDPR' (*edri.org*) <https://edri.org/our-work/open-letter-edri-urges-enforcement-and-actions-for-the-2-year-anniversary-of-the-gdpr/> accessed 2 November 2021; Electronic Privacy Information Center (EPIC), 'Feedback from: The Electronic Privacy Information Center (EPIC)' (6 August 2021) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665484_en> accessed 17 November 2021.

and may be injected or further expanded into the current assessment procedure to improve its efficiency. The analysis has also spotlighted some of the positive features of the DPIA that are of particular value and should be further emphasized.

Starting from the positive notes, there are two strong aspects of the DPIA model. First the fact that the assessment is a binding requirement and is not implemented simply on a voluntary basis, like most of the other proposed IAs. This is an important aspect as it provides the assessment a solid legal basis that should support its easier and general enforcement. Second, the process adopts an *ex-ante* assessment approach subject to *continuous updating*. Hence, unlike other IAs (e.g., HRIA)[1376] that may be carried out even after the activity's deployment, the DPIA has the precise objective to investigate and address the possible impacts prior to their realization, and ensure that the envisaged risks and the implemented mitigating measures remain accurate in the course of time. While the continuity aspect is mentioned both in the GDPR[1377] and in WP29 guidelines[1378], the speed with which processes and data practices transform requires to stress its importance, so that DPIA updates are normalized as part of controllers' internal compliance review process.

As for the "improvable" aspects, several lessons can be drawn from the above exploration.

(i) A first aspect that emerges, particularly from the analysis of ETiA and HRIA, as well as their variations, is the broad understanding of the notion of "risk" adopted by these models, which is defined against a wide range of rights and values that help to assess the impacts not only at an individual but also social and collective level. As mentioned above, despite the language of the GDPR, currently the scope of risks acknowledged in a DPIA remains very limited[1379]. Rebranding the DPIA as an assessment that addresses impacts in a comprehensive manner, thus incorporating a deeper human rights and ethical sensitivity, makes it not only more consistent with the wording of the GDPR, but it allows to strengthen its ability to effectively protect individuals from data

[1376] See Moss and others (n 1348) 20 and 54., discussing about the different "time frames" of different IA models.
[1377] Art. 35(11) GDPR.
[1378] Article 29 Data Protection Working Party, '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' (n 427) 14.
[1379] Mantelero, 'AI and Big Data' (n 1293) 761; Kaminski and Malgieri (n 1347) 136; Gonçalves (n 1294) 6.

processing risks[1380]. On the one hand, this would force controllers to engage in a reasoned analysis of the multiple factors involved, avoiding it to become a mere formalistic exercise. On the other hand, only this type of evaluation allows to consider the impacts of an intended activity from different angles, thus ensuring that the safeguards implemented to mitigate the detected (individual and social) risks do in fact provide the fullest possible coverage. As noted, when the scope of the assessment expands, the complexity for controllers to identify in practice the values and issues on which to focus remains one of the stumbling blocks for the adoption of the assessment[1381]. Harmonized sectoral and context-related instructions (see *infra* point v), the involvement of experts (see *infra* point ii) and specific coordinated guidance by the EPDB/DPAs are necessary components to support the success of the model.

(ii) A second evident shortcoming of the DPIA model is the absence of mandatory participatory mechanisms to engage stakeholders, which is on the contrary one of the key aspects of the alternative IA models. Consultation with stakeholders helps to give a voice to concerned individuals and groups; to better understand the competing values at play and to flag critical underestimated issues[1382]. A more effective assessment model should thus contemplate a better involvement of concerned individuals, not limited to general surveys sent to users, as already advised by the WP29[1383], but mostly through the engagement of NGOs and other representative organizations, both more experienced and knowledgeable than individuals. The involvement of experts, to obtain technical, legal, ethical and social inputs to help correctly frame the discussion would also improve the quality and accuracy of the DPIA process[1384]. This does not mean that any DPIA, regardless of the type of processing, should require external input as a rule. DPAs (as well as other civil society actors) should both incentivize stakeholders' engagement but also provide guidance to support controllers in determining the factors/activities for which external consultations are highly recommended.

(iii) The implementation of adequate oversight mechanisms is a further essential element of impact assessment, which is currently lacking in the DPIA procedure. Some have rightfully advocated for the reinforcement of the role of supervisory authorities in

[1380] Lindblad Kernell, Bloch Veiberg and Jacquot (n 1344) 39–40.
[1381] Raab (n 1276) 13.
[1382] Mantelero, 'AI and Big Data' (n 1293) 769; Lindblad Kernell, Bloch Veiberg and Jacquot (n 1344) 10.
[1383] Article 29 Data Protection Working Party, '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' (n 427) 15.
[1384] Gonçalves (n 285) 9.

the prior assessment of data processing[1385]. However, the limited GDPR rules on prior consultation and, mostly, cost-efficiency reasons lead to conclude that a greater involvement of DPAs, both in the assessment and enforcement phases, is not realistic. This said, it may be sufficient a higher number of enforcement actions dealing with DPIAs compliance to create a good resonance not only to prompt better compliance, but also to identify recurring issues to be addressed on a more general level[1386]. Further efforts in this sense are still to be expected from DPAs.

As seen in other IAs, alternative mechanisms that make use of third-party actors to perform decentralized oversight functions are available, none of which, however, is duly harnessed under the GDPR framework.

The absence of public disclosure requirements of the assessment results has been pointed at as one of the biggest shortcomings of the DPIA[1387]. The WP29 ranks the publishing of the DPIA as a simple "good practice" that remains up to the controller's decision[1388]. As a result, the voluntary practice of disclosing DPIAs assessment has never flourished, with great drawbacks in terms of transparency and lack of public oversight. The publication of the assessment procedure's outcomes, in fact, prompts public feedback and enables collaborative governance, by providing civil society actors with new means to carry out their monitoring activities[1389]. Releasing a summary of the DPIA assessment or different layers of information depending on the targeted audience[1390], may be sufficient to trigger the mechanisms mentioned above. In order to improve the effectiveness of the DPIA procedure and prevent the reinstatement of a "tick-box" approach, imposing stronger disclosure requirements is imperative. Similarly, the institutionalization of third-party oversight mechanisms and other independent-expert review (e.g., algorithmic auditing)[1391], to activate *ex post* when the DPIA drafting or update has been finalized to verify its compliance, is a further component that would support the overall governance regime.

[1385] Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (n 586) 654–659.
[1386] Kaminski and Malgieri (n 1347) 140.
[1387] Reisman and others (n 1347) 13.
[1388] Article 29 Data Protection Working Party, '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' (n 427) 18.
[1389] Kaminski and Malgieri (n 1347) 130.
[1390] Mantelero, 'AI and Big Data' (n 1293) 766.
[1391] Moss and others (n 1348) 48; Reisman and others (n 1347) 18.

(iv) Beyond the limited (but significant) enforcement function that DPAs should exercise to improve DPIAs effectiveness, discussed above, the guidance role of DPAs in the context of impact assessments should also be more incisive. Supervisory authorities may play a fundamental part in establishing concrete best practices and context-specific guidelines to facilitate controllers in the performance of sector DPIAs[1392]; in clarifying and better framing the participation requirements of stakeholders in the DPIA procedure[1393].

5 Introduction of "hard boundaries"

The doctrinal debate has at time voiced authors that considered with favour the adoption of strict paternalistic measures, namely "hard regulatory boundaries" to prohibit, at the outset, particularly troublesome data processing practices or improper uses of personal data[1394]. In their view, the fundamental inability of data subjects to exercise their subjective rights exposes both them and, as a consequence, society to the possible threats of data processing activities. Even the adoption of "softer" paternalistic measures, explored previously in this work[1395], leaves too much to the individuals' choice to be considered an effective option when the resulting harms are evident and systemic.

The positions supporting stronger prohibitions over data uses have been usually contrasted by the arguments of those warning against the risks of over-paternalism, already touched upon previously in this work[1396], particularly stressing the contextual nature of processing activities and the difficulties of establishing harm-based rules in the privacy context.

Indeed, EU data protection law appears to have embraced the latter view. Even though traditionally the EU approach to data protection has been more paternalistic, relatively

[1392] Kaminski and Malgieri (n 1347) 140.
[1393] Gonçalves (n 1294) 10.
[1394] Fred H Cate, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer protection in the age of the 'information economy'* (Ashgate 2006) 343; Anita L Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press 2011); Fred H Cate and Viktor Mayer-Schonberger, 'Notice and Consent in a World of Big Data' (2013) 3 International Data Privacy Law 67, 69; Solove, 'Privacy Self-Management and the Consent Dilemma' (n 12) 1903; Borgeswius (n 576) par. 9.7; Claudia Quelle, 'Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps*, vol 498 (Springer International Publishing 2016); Amber Sinha, 'A Case for Greater Privacy Paternalism? — The Centre for Internet and Society' *The Center for Internet & Society* (14 February 2016) <https://cis-india.org/internet-governance/blog/a-case-for-greater-privacy-paternalism#_ftnref16> accessed 1 December 2021.
[1395] See Chapter III, par. 2.2.
[1396] See Chapter III, par. 4.

speaking, than the hyper-libertarian approach adopted in the US legal system, even EU law has not gone as far as including general rules banning the performance of specific data processing activities[1397]. The "purpose limitation principle" seems to be the only indication in the GDPR that takes into account the use (purpose) that data are put to. Yet, it offers only generic guidance regarding the type of purposes allowed, namely "legitimate" purposes, to be interpreted as meaning compliant with the law in the broadest term)[1398]. Beside the fact that such an abstract wording, which assumes controllers should determine in practice whether a use is lawful or not, is neither realistic nor effective, the harms stemming from processing activities may neither be obviously unlawful from the outset (e.g., the case of "hidden" discriminations), nor clearly fall under the scope of specific rules under EU or national laws (e.g., processing leading to manipulative outcomes or discriminatory outcomes that fall outside traditional non-discrimination law cases)[1399].

When the GDPR acknowledges the possibility of "banning" certain processing operations, these bans result from an exercise of corrective powers by supervisory authorities, which according to the GDPR have the faculty to «impose a temporary or definitive limitation including a ban on processing»[1400]. Hence, again this type of prohibition has no generalized and preventive character. National DPAs, in fact, exercise this type of action as an urgent temporary measure to prevent immediate threats pending a proceeding[1401], or as an addition to a pecuniary measure in cases of established violations of GDPR provisions, to prevent the perpetration of the infringing activity[1402]. This form of prohibition has therefore a limited scope: it applies usually after

[1397] Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 Law, Innovation and Technology 266, under par. 3.2.
[1398] Article 29 Data Protection Working Party, 'Opinion 3/2013 on Purpose Limitation' (2 April 2013) WP203 19, connected to the general requirements of "lawfulness" and "fairness" under Art. 5(1).
[1399] Frederik J Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 The International Journal of Human Rights 1572; Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' (n 1190). For example, when algorithms do not produce discriminatory treatments based on the traditional protected classes of non-discrimination law (like gender, ethnicity, sexual orientation), rather use "new classes" (such as financial situation; postal code; or a specific habit).
[1400] Art. 58(2)(f) GDPR.
[1401] See for example the decision of the Italian DPA that imposed an immediate limitation on the processing performed by TikTok with regard to the data of users whose age could not be established with certainty, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9508923; see also the attempt of the Hamburg DPA to ban further processing of WhatsApp users' data by Facebook https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung.
[1402] See e.g., the many decisions of the Italian DPA against telecom companies where, alongside an administrative fine, it permanently limited certain data processing for marketing purposes, Tim: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9256486; Wind:

the potentially harmful activity has already taken place and it has no general application, as it results from a case-by-case assessment.

Even when it appears that the GDPR introduces certain prohibitions (e.g., Art. 9 on particular categories of data[1403]; or Art. 22 on individual automated-decision making and profiling[1404]), it still leaves a consistent list of derogations[1405] (all which include the data subject's consent) that allow to circumvent the prohibition and carry out the data processing anyway. The same approach is adopted with reference to the forthcoming e-Privacy Regulation[1406] that although includes an express prohibition to certain processing activities (e.g., users' tracking), as opposed to the current more permissive e-Privacy Directive, exceptions are always present, in particular the data subject consent[1407].

In sum, traditionally, data protection law lays down the conditions under which data can be processed (e.g., data subject's consent), introduces transparency requirements to permit to verify that the conditions are met and defers the assessment of the concrete risks of the processing activity to the data controller.

5.1 Introduction of tailored prohibitions on data uses and practices

Against this background, however, there is an increasing emergence of practices (particularly in connection to intrusive profiling and the use of AI techniques) that have worrying and significant impacts on individuals and society. Predictive analytics may increasingly lead to unknown and uncontrolled discriminatory outcomes, without individuals having any awareness or control[1408]. Pervasive tracking, behavioural profiling and microtargeting of individuals are exponentially used with manipulative

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753; Vodafone: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9485681 .

[1403] Art. 9(1) GDPR states: «processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited».

[1404] Art. 22(1) GDPR reads: «the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her», which has been interpreted as a general prohibition for automated-decision making. Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 478).

[1405] Art. 9(1) GDPR and Art. 22(2) GDPR.

[1406] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (n 324). The draft regulation is still in the process of being finalized and, when it will enter into force, it will replace the currently applicable e-privacy Directive.

[1407] E.g., Art. 8(1) of the proposal for an e-Privacy Regulation.

[1408] Mühlhoff (n 635). and more extensively in Chapter II, par. 3.2 above.

intents, exploiting individuals' vulnerabilities, emotions and inclinations, both for commercial and non-commercial purposes[1409]. Tangible and extensive negative effects stemming from data uses without equal improvements in the ability of data subjects to anticipate and contrast this type of dangers call for a revision of the current approach. Relying on *ex post* monitoring and enforcement activities of DPAs and NGOs or *ex-ante* "enhanced" forms of impact assessments on case-by-case data processing operations may not be enough when the threats that processing practices present for both individuals and society are particularly serious and pervasive.

In these cases, a more radical approach that introduced restrictions and prohibitions on certain specific data practices may be considered a viable option. While the adoption of an overly paternalistic system of bans and authorizations to data processing is neither feasible, nor appropriate, EU policymakers should start to develop a clearer position on the merits of processing activities. Stronger decisions on which data uses are aligned with individual and societal interests and which are not, to determine acceptable and permitted processing, needs to be taken. And, whereas the contextual nature of data processing makes this assessment incredibly complex and filled with trade-offs, an agreement should be at least achieved on those processing activities that are deemed to be most threatening and dangerous for individuals and society.

An interventionist approach, along the lines indicated above, has in reality begun to surface in the context of certain legislative proposals currently discussed at EU level, in the context of the European Digital Strategy[1410]. While not directly affecting existing privacy rules, these proposals move in the direction of introducing specific prohibitions for certain data practices and uses, thus in practice supplementing the current data protection framework with *ad hoc* paternalistic restrictions.

The discussion has been particularly animated with reference to the topic of "targeted advertisement" in the context of the proposal of the Digital Services Act (DSA)[1411], introduced alongside the Digital Markets Act (DMA)[1412] in December 2020, as part of

[1409] European Data Protection Supervisor, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (n 613). The Cambridge Analytica scandal has publicly revealed the use of profiling techniques to micro-target voters for political purposes. Hern (n 633).
[1410] European Digital Strategy: https://digital-strategy.ec.europa.eu/en/policies .
[1411] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (2020) COM/2020/825 final.
[1412] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' (2020) COM/2020/842 final.

the EU legislative package to update rules for digital services. Objective of the DSA is to set out new harmonized rules for online intermediaries offering their services in the EU single market, tackling issues connected to online illegal and harmful contents, service providers' liability regime and transparency and safety of the online environment[1413]. While data protection is not a core-objective of the DSA, it does introduce provisions that directly affect the processing of users' personal data, complementing the data protection provisions of the GDPR.

A set of rules that has sparked quite a debate regards provisions that regulate *targeted online advertisement*, that different actors have criticized as too soft, calling for the introduction of stricter prohibitions on such activities.

Among these actors, the European Data Protection Supervisor (EDPS) has taken a strong stance on the matter, urging the introduction of a proper *ban on surveillance-based targeted advertisement*. The position of the EDPS follows and strengthen the request for tighter rules previously made by the EU Parliament with reference to the ad-tech industry[1414]. In its 2021 February Opinion, the EDPS recognizes that «certain activities in the context of online platforms present increasing risks not only for the rights of individuals, but for society as a whole»[1415], particularly with reference to the risk of manipulation associated with online targeted advertising[1416]. In this regard, the EDPS has supported the introduction of stricter rules for less intrusive forms of advertising and has urged the co-legislator to consider additional requirements beyond transparency. These measures should include a «*phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking*»[1417] and restrictions in relation to the categories of data that can be processed for targeting purposes and disclosed to

[1413] For an overview of the DSA see: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[1414] In particular, European Parliament, 'European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on the Digital Services Act: Improving the Functioning of the Single Market' (2020) P9_TA(2020)0272.

[1415] European Data Protection Supervisor, 'Opinion 1/2021 on the Proposal for a Digital Services Act' (10 February 2021) 6.

[1416] European Data Protection Supervisor, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (n 613). Also, the DSA proposal mentions under Recital 63 «illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality».

[1417] European Data Protection Supervisor, 'Opinion 1/2021 on the Proposal for a Digital Services Act' (n 1415) 16. The position has been more recently upheld also by the EDPB, European Data Protection Board, 'Statement on the Digital Services Package and Data Strategy' (18 November 2021) 2–3.

advertisers or third parties to enable or facilitate targeted advertising[1418]. With this affirmation, the EDPS takes a very strong stance that goes beyond previous more cautious positions on the matter. Compared to advices submitted in previous occasions (e.g., on tracking practices and profiling of individuals[1419]), the EDPS moves towards supporting a full prohibition of specific processing activities, leaving no margin of manoeuvre for neither controllers nor data subjects.

This position has been also voiced in the more recent Opinion[1420] of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), adopted in July 2021 that includes among its key proposal a specific *prohibition on surveillance-based targeting*. In the words of the LIBE Committee «misleading or obscure advertising for non-commercial and political purposes is a special class of online threat because it influences the core mechanisms that enable the functioning of our democratic society»[1421]. For this reason, it amended the current proposal so that behavioural and personalized targeting for *political and other non-commercial purposes* become expressly prohibited and extended the same targeting restrictions should apply to minors or on the basis of special categories of data which allow for targeting vulnerable groups[1422].

The acknowledgment of individual and societal risks involved in modern data processing practices that require more than self-governance mechanisms and individual control is expressed also in a study commissioned by the European Parliament on the regulation of targeted and behavioural advertisement[1423]. After analysing the ways in which the advertisement sector operates and reviewing the rules that govern the collection and processing of personal data to feed the ad machine, the authors recognize quite bluntly that «the implementation of the idea that consent should be free unfortunately is likely to be insufficient to take data subjects out of their

[1418] European Data Protection Supervisor, 'Opinion 1/2021 on the Proposal for a Digital Services Act' (n 1415) 16.
[1419] See e.g., the recommendations in European Data Protection Supervisor, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (n 613); European Data Protection Supervisor, 'Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (EPrivacy Regulation)' (24 April 2017).
[1420] Committee on Civil Liberties, Justice and Home Affairs (LIBE), 'Opinion on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (2021) PE692.898v07.
[1421] ibid amendment to recital 15(b), 13.
[1422] ibid amendment to Art. 2(b), 46.
[1423] Sartor, Lagioia and Galli (n 613).

predicament»[1424] and that «even if this idea is implemented in stringent and effective ways, it remains true that most people do not have the competence, or in any case the time to understand data-protection options and engage in meaningful choices»[1425]. They do not abandon completely the idea of "free and informed consent", however, alongside measure to maximize the individual right to choose, they also propose to «restrict the extent to which consent can be traded for services or other counter-performance»[1426], essentially making certain type of processing activities unlawful. In particular, they propose to exclude the efficacy of consent for targeted advertising for political rather than commercial goals (e.g., for targeted electoral propaganda) and for processing that «may be considered too risky, or anyway incompatible with data protection principles», such as the use of third-party cookies for purpose of targeted advertising, mechanisms such as real time bidding, or the processing of sensitive data[1427].

A similar protective approach, although from a different angle, can be read in the newly proposed draft of the EU Commission for a Regulation on Artificial Intelligence (AI Act)[1428], which sets a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values, fundamental rights and principles.

AI systems are fundamentally data-driven systems, they do not necessarily feed on personal data but, as emphasized by the EDPS-EDPB, the development and use of AI systems «in many cases involve the processing of personal data»[1429], they may involve profiling and automated-decision making processes[1430]. So far, AI has fallen under the umbrella of the GDPR that regulates its applications but, as clarified above, does not prohibit any processing activity or practices from the outset.

[1424] ibid 122.
[1425] ibid.
[1426] ibid 117.
[1427] ibid 118.
[1428] European Commission, 'Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (n 764).
[1429] European Data Protection Supervisor - European Data Protection Board, 'Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (18 June 2021) 9.
[1430] Further on the relationship between profiling, automated decision-making and AI Information Commissioner's Office (ICO), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection v. 2.2' (2017).

It seems that this will change under the new AI-Regulation. Like the GDPR, the AI Act follows a risk-based approach and imposes regulatory burdens when AI systems are likely to pose high risks to fundamental rights and safety, subject to case-by-case assessments. However, contrary to data protection law, the Proposal includes also a list of *prohibited AI practices*[1431], where the level of risk is considered «unacceptable» as «contravening Union values, for instance by violating fundamental rights»[1432]. In the latter cases, the policymaker does not leave room for contextualization and mitigation, and simply declares the practices too risky for individuals, groups or the society at large to be permitted. The list contains prohibitions that cover practices that have a significant potential to manipulate persons (their behaviour, opinions, decisions) through subliminal techniques beyond their consciousness[1433] or that exploit their vulnerabilities (based on age, physical or mental capacities) to cause harm[1434], that evaluate or classify the trustworthiness of natural persons based on their social behaviour or personal characteristics ("social scoring")[1435] and real-time remote biometric identification systems[1436]. The EDPS and EDPB in a joint preliminary opinion on the AI Act[1437], as well as other early commentators on the proposal[1438], have welcomed the recognition of "unacceptable AI" and called for even stricter rules to encompass broader categories of prohibited AI and better specify some of the criteria.

It is too soon to anticipate how the final version of the current Proposal will look like and whether the provisions banning AI uses will be broadened or narrowed. However, it is reasonable to expect that this precautionary approach will be maintained.

By prohibiting the deployment and use of specific AI systems, the provision does indirectly exclude the legitimacy of certain profiling and automated decision-making practices, at the basis of those systems, removing any margin of choice from the individual or the user of those system (i.e., the data controller).

[1431] The list is included under Art. 5 of the AI Act.
[1432] See par. 5.2.2. of the Proposal's Explanatory Memorandum and Recital 15: «Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child».
[1433] Art. 5(1)(a) AI Act.
[1434] Art. 5(1)(b) AI Act.
[1435] Art. 5(1)(c) AI Act, when the social score is detrimental or unfavorable to individuals.
[1436] Art. 5(1)(d) AI Act.
[1437] European Data Protection Supervisor - European Data Protection Board (n 1429).
[1438] See Edri European Data Protection Supervisor - European Data Protection Board (n 481)., Algorithmic Watch https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/ .

5.2 Concluding remarks

The introduction of substantive rules to restrict or prohibit certain processing practice may be considered as excessively paternalistic. It inevitably limits data subjects' personal agency over the sharing and use of their data.

At the same time, the severity and pervasiveness of the threats posed by certain data processing and practices, both for individuals and society at large, calls for a more incisive action to prevent these activities from being permitted in the first place, rather than sanctioned when its effects have already occurred.

6 Conclusions

The investigation conducted in this chapter has attempted to provide a further layer of detail to the analysis, exploring additional mechanisms that could be leveraged to compensate for the protection gaps that cannot be effectively filled simply relying on individuals' capacities.

Contrary to the individual-centric measures, considered under Chapter III, the different options analysed in this chapter move away from the data subject sphere of control and make use of the expertise, resources and powers of other societal actors.

Below there is a schematic summary of the main findings of the above analysis.

Response	Effects	Issues
Boosting DPAs	- Investigatory powers to perform in-depth monitoring of processing activities (also thanks to possibility of international cooperation) - Expertise and independence to assess the risks of processing practices (both at individual and collective level) - Incisive enforcement powers to ensure compliance with data protection rules - Educational role to promote awareness and support individuals	- Mainly ex-post monitoring mechanism (little ex-ante overview) - Lack of resources and staff - Poor enforcement
Leveraging NGOs and other societal actors	- Skills to perform a widespread oversight on data processing practices	- Poor and burdensome instruments to exercise independent monitoring functions

	- Expertise to conduct in-depth scrutiny on controllers' activities and hidden data processing - Educational role to support individuals - Mobilizing effect and public pressure to raise public awareness on sensitive data processing topics and prompt compliance	- Weak synergies among societal actors - Little consideration from DPAs
Collective management solutions	- Take care of the micro-management of privacy rights in the interest of data subjects - Expertise to better assess (ex-ante) the consequences of processing activities - Better positioned to negotiate with data controllers and monitor their subsequent activities	- Solutions still in their infancy - Open questions on: legal and technological structure of these new intermediaries; compatibility with GDPR framework; successful dissemination
Reinforcing DPIA process	- *Ex-ante* assessment and mitigation of the impacts (both at individual and collective level) of processing activity before they are put into place, ensured by: (1) comprehensive scope of the assessment process; (2) involvement in the assessment process of data subjects and third-party independent actors (e.g., NGOs and other representative entities) that act in the interest of data subjects; (3) introduction of third-party oversight mechanisms + mandatory disclosure of DPIA outcomes.	- Requires a deep cultural change with respect to how controllers currently approach DPIAs and the commitment of different societal actors - Burdensome and expensive process that requires expertise and resources - Lack of sectorial-specific guidelines to facilitate the conduction of tailored DPIAs - Lack of proper monitoring and enforcement activities on how DPIAs are conducted
Introduction of "hard boundaries" to data uses	- Upfront prohibition of certain data uses, considered particularly dangerous for individuals and society	- Complicated assessment to determine what data uses should be banned from the outset - Requires EU-wide public debate and serious policy commitment

Table 12. Mechanisms to supplement individual control

The heterogeneous set of measures considered above does not intend to fully replace the individual control model with a strong paternalistic approach to data protection. Even when more interventionist measures have been proposed (e.g., the introduction of rules banning certain data uses) that do indeed in some form limit individuals' freedom of decision, these should be employed in a "tailored" fashion only as exceptional outer boundaries for the most evident data abuses.

These mechanisms build a structured and responsive support network around individuals, that, on the one hand, helps them to safeguard the effective and aware exercise of their subjective rights from the abuses and hidden manipulations of controllers; on the other hand, supplement the inevitably limited evaluation and oversight capabilities of individuals to protect both individuals themselves and society more generally from dangers they would not be able alone to prevent.

The analysis has shown the advantages, in terms of better oversight, assessment and public control over processing practices, that could derive from an active engagement of a broader ecosystem of actors that already populates the data protection world, but it has also underlined some of its current limits.

Indeed, compared to the measures analysed in the previous chapters, the effective implementation and improvement of the mechanisms presented in this chapter require bigger and long-term efforts. However, given the serious problems individuals experience today in controlling the use and circulation of their personal information and the limited improvements offered by new subjective rights and technologies, the promotion and valorization of mechanisms that operate beyond a strictly individual-centric dimension is critical to build a systemic and comprehensive response to these issues.

CONCLUSIONS

This work has developed around the widely emphasized concept of “individual control over personal data”, deemed an essential principle for the empowerment of data subjects, in an attempt to investigate its effectiveness and feasibility in an increasingly digitized and datafied society.

To this purpose, the analysis has first provided a *historical overview of the emergence of this notion* in the European data protection context, taking into account its role in the doctrinal debate, its legal manifestation within regulatory provisions (at national, international and EU level) and the approach of the CJEU jurisprudence on the matter. The investigation has revealed that the idea of individuals being in control of their personal data and active participants in their management has progressively emerged as a core component of data protection. The connection between data protection and the safeguard of individual rights such as identity, autonomy, self-development and self-determination supported the view that the ability of individuals to keep control over their personal data, as information bits of their own “Self”, was a key expression of those underlying values. Upon these premises, the subjective understanding of control, at times identified with the German-based concept of “informational self-determination”, has continuously strengthened, establishing itself as a central pillar of European data protection laws.

Despite its centrality, the analysis has also pointed out how a general principle of “individual control” has not been established in the EU framework, nor has been directly recognized as such in the CJEU case-law. Instead, the concept has manifested obliquely as a bulk of subjective powers and rights that, together, should provide individuals with the instruments to exert control in terms of deciding, managing and monitoring the use and circulation of their personal information. The “empowerment” of data subjects has thus been defined by the progressive increase and expansion of individual rights, headed by “notice & consent” rules, primary representation of self-determination and decisional autonomy, and further followed by a number of other rights that endow individuals with specific entitlements over their personal data (to access, erase, rectify, ask for the portability or not being subject to an automated decision-making process).

Further, the analysis has explored the manifold *issues that undermine* the effective implementation of this idea of *individual control*, also as a result of the technological developments that have transformed our society and revolutionized the way in which we live and communicate. Human cognitive limitations and biases substantially affect individuals' level of engagement and comprehension when it comes to privacy matters (due to notice fatigue, time constraints, over-complexity and language technicality). When it comes to privacy-related choices, the skewed rationality of individuals (i.e., "bounded rationality") impairs their assessment and oversight capacities, exposing them to consequences they did not understand or even expect. The combined effects of phenomena like big data, advanced analytics, IoT, algorithmic profiling and AI have only made things bigger, more complex and more expensive and time-consuming to handle. The network of stakeholders engaged in data collection, exchange and processing has achieved such an impressive scale that data subjects have no means to keep it under track. Big data and advanced algorithmic processes have also improved profiling capacities to such an extent that individuals often have no clue about the type of information that may be inferred and predicted about them, and what impacts they may suffer as a result. The intricacy and obscurity of these technologies make the technical application of safeguard measures (e.g., "human intervention") particularly troublesome. In addition, impediments arising from debated interpretations on the legal scope and application of newly introduced rights (like the right not to be subject to solely automated decisions or the right to data portability) have created additional barriers to their effective exercise. In summary, multiple factors, whether cognitive, technological or legal, currently affect the ability of individuals to pursue and protect their privacy interests.

In addition, the analysis has emphasized how the myopia that characterizes the privacy self-management logic does not affect only individual privacy interests, but it translates also into a lack of consideration for the externalities that individual privacy choices may have on the collectivity and society at large. First, privacy and data protection have a social function that transcends the achievement of strictly personal interests and directly connects to the "quality" of a democratic society itself, hence to the protection of values (e.g., free and fair elections; equality and non-discrimination; non-pervasive and unlawful surveillance) that have proven to be jeopardized by (mis)uses of personal data. Secondly, technological advances have dramatically increased the possibility of making

predictions and inferring information about an individual, based on personal data disclosed by hundreds of others. Group profiling resulting from the mass-analysis of information provided by a number of people, in fact, enables controllers to assess, rank and take decisions (with potentially discriminatory or biased effects) on other individuals that have not contributed to create the profile, but share with the original members of the group certain characteristics. When individuals decide to share their data, consent to certain data processing, or exercise their subjective rights, however, they act on a strictly individual-centric basis that focuses on their individual privacy preferences, but remain blind to the broader collective impacts that their decisions may entail.

Despite the long list of shortcomings that impinge on the effective and successful exercise of control prompts a serious reflection on the place that this approach to data protection is assigned in today's digital society, it has also been argued that a radical abandonment of the idea of individual control should not be taken as the definitive solution to these issues. The ability of people to take decisions, manage and monitor how others access, share and use their personal data is a fundamental expression of their rights to identity, autonomy and self-determination, which remain values at the core of data protection essence and objectives. Therefore, the right of individuals to "have a say" on their personal data needs to be safeguarded, even though possibly downsized, to ensure them a minimum space of autonomy.

The analysis makes it clear: there is unfortunately no silver bullet. There is no one-fit-for-all solution that can effectively deal with and solve the manifold issues of the privacy self-management logic. The issues raised by individual control are varied and systemic, therefore only a multifaceted and systemic response may hope to be effective in tackling these shortcomings.

In particular, the work suggests that, to move forward, appropriate actions should be taken moving along *two directions*.

On the one hand, greater efforts should be made to encourage and leverage supporting measures that, taking into account the current technological and social context, can assist individuals by reinforcing and adjusting their control capacities to the new digital needs. From this perspective, the work has identified a number of options, both in the technological and legal field, that should be better expanded and deployed to improve the individual control toolkit. Technical solutions, like PETs, have a great but yet to

develop potential. They help to tackle the complexity and ubiquity of the current data ecosystem, providing data subjects with technologies (e.g., data stores), that should assist individuals in an easier micro-management of their privacy choices and subjective rights. User-friendly nudging interventions, whether in a softer version of “legal design” approaches or in a more intense form of defaults and incentives, should also be given further thoughts. When successfully implemented, these types of measures may in fact improve the background against which individuals adopt their privacy decisions and gently guide users, without depriving them of their decisional autonomy, into making more informed and better choices. From a legal standpoint, scholars have also suggested the introduction of “new” rights, to enrich the catalogue of legal means that users could exercise vis-à-vis controllers with instruments better tailored to the evolving data-driven context. Even though these solutions appear to be less promising, both in terms of practical application and envisaged effectiveness than the technically-oriented solutions described above, they should nonetheless be further explored. Some proposals (e.g., introduction of an *ex-post* “right to explanation” of algorithmic-based decisions), more than others (e.g., establishment of a “right to property” on personal data), may also play a part in enhancing the position of data subjects vis-à-vis controllers.

On the other hand, the analysis has pointed out how providing individuals with better and stronger tools does not solve all the shortcomings that the model of individual control currently suffers. It should be accepted that individuals remain, in many cases, poorly equipped to deal alone with the intricacies of the modern data processing environment. Efforts should therefore also be put in strengthening measures that are less “individual-centric”, in that they both engage different societal actors (than data subjects) and address data protection from a broader collective perspective.

As the work underlines, the current EU data protection framework does already include a number of mechanisms that may contribute, each in their own way, to build a “safety net” around individuals to help them exercise their rights in a genuine manner, but also fill the protection gaps left by some of the intrinsic and insuperable limits of the privacy-self management logic. The latter are, however, not sufficiently strong or adequately leveraged to compensate for individuals’ deficiencies, therefore better efforts should be placed in this sense. In addition, other approaches, even though not formally endorsed

or fully operative yet, are also starting to come forth as viable alternatives to compensate for some of the identified shortcomings.

In particular, the analysis has shown the essential role that a healthy and responsive "architecture of empowerment", formed by entities (supervisory authorities, NGOs, representative organizations, activists and academics) that operate as guardians and allies of individuals, may play in the data protection context, if sufficiently supported and expanded. All these entities, in fact, are in principle equipped with the technical expertise and means to scrutinize and shed light on the activities of data controllers, as well as better understand and assess the data processing operations they carry out. In doing so, these actors are better placed to monitor controllers' behaviours and prevent them from obstructing or manipulating individuals' attempts to exercise their control rights, but are also better skilled to assess the possibly long-term or hidden consequences of processing activities, both at individual and collective level. What they often lack are adequate resources to perform their tasks and strong network synergies to mutually reinforce and take advantage of each other's efforts, both issues which should be adequately and urgently addressed. The educational and awareness functions that these subjects serve should also be better emphasized, as they help to form active citizens and raise public attention on the most urgent societal topics. Finally, the means these actors can rely on to enforce compliance, not only through hard enforcement and corrective actions but also media exposure and public pressure, should also be further strengthened.

In this same context of existing but poorly leveraged mechanisms, the analysis has also shown the advantages that may result from the adoption of "improved" versions of DPIAs to prevent from the outset processing activities bearing significant risks for individuals and society. The overview of other types of *ex-ante* impact assessments, employed in different fields, have highlighted the merits and limits of the current DPIA version and offered useful insights for its improvement. Notably, placing emphasis on the comprehensive scope of the assessment (to incorporate a deeper human rights and ethical sensitivity); a better engagement of sector experts and digital rights organizations during the assessment process; public disclosure of DPIA's results; introduction of third-party auditing mechanisms and the issuing of context-based instructions and models to provide standard sector-specific base lines for the

conduction of DPIAs, are all elements that may upgrade and refine this type of instrument.

On the emerging options' side, solutions that enable a collective and mediated management of subjective rights, especially in the form of new data governance models such as "data trusts" and "data cooperatives", also offer promising cues. These solutions have the advantage of introducing qualified intermediaries that, acting on individuals' behalf and in their interest, replace them in the burdensome micro-management of their personal data. In addition, the centralized and collective management of data belonging to a community of members would enable the establishment of new "data agglomerates", this time on the side of data subjects, that may help to rebalance existing power dynamics and empower data subjects against big platforms and other data collectors.

Finally, the adoption of "hard boundaries" on certain data processing activities is an option that should be given more consideration. Even though scholars have generally advised against over-paternalistic regulatory interventions, the consequences that certain data practices generate have become so impactful and dangerous that relying simply on *ex-post* monitoring and *ex-ante* self-governance tools appears to be increasingly insufficient. A moderate approach based on the introduction of tailored prohibitions on certain data uses would provide a generalized response to those data processing that may have consequences particularly dangerous and harmful for individuals and society at large, and should therefore be banned from the outset, leaving no leeway for individuals or controllers. Some recent legislative proposals seem to slowly move in this direction.

In conclusion, each of the described measures is alone not sufficient to fully restore individual control, nor to compensate for its most evident weaknesses. Also, each of these solutions bears its own share of challenges.

However, the promotion and valorisation of the proposed mechanisms and the combined benefits that these could bring, in their own way, on the data protection table are a first essential step to start building a systemic response to the protection gaps that afflict individuals and society as a result of the weaknesses currently affecting the individual control logic. In the end, it is true when they say «many hands make light work».

Bibliography

National and international acts

Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954) (German Federal Data Protection Act – BDSG 1990)

Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (*Datenschutzgesetz* - DSG). BGBl. Nr. 565/1978 (Austrian Data Protection Act -DSG)

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', 1981 (Convention 108)

——, 'Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data', 2017

——, Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 1973

——, Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 1974

Datalag (1973:289), Svensk författningssamling, 11.05.1973 (Swedish Data Act)

Datenschutzgesetz (GVBl. II 300-10) vom 7. Oktober 1970 (Hessen Data Protection Act)

Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (*Bundesdatenschutzgesetz* – BDSG) vom 27. Januar 1977, in der Fassung der Bekanntmachung vom 1. Februar 1977 (BGBl. I Nr. 7 S. 201) (German Federal Data Protection Act - BDSG)

Henkilörekisterilaki 471/1987 (Finnish Personal Data Register Act)

Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (French Loi informatique *et Libertè*)

Lov om personregistre m.m. (LOV-1978-06-09-48) (Norwegian Personal Register Act)

Organization for Economic Cooperation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 1980 (1980 OECD Guidelines)

UK Data Protection Act, 1984 (UK Data Protection Act)

Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 18 maart 1992 (Belgian Data Protection Act)

EU primary and secondary law

Charter of Fundamental Rights of the European Union (EU Charter)

Directive 2002/58/EC (e-privacy Directive)

Directive 95/46/EC (DPD)

Regulation (EU) 2016/679 (GDPR)

Other EU level acts

European Commission, 'Commission Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (87AD) 81/679/EEC

——, 'Completing the Internal Market — White Paper from the Commission to the European Council' (1985) COM (85) 310 final

——, 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data' (1990) COM/90/314FINAL-SYN 287

——, 'Report from the Commission. First Report on the Implementation of the Data Protection Directive (95/46/EC)' (2003) COM(2003) 265 final

——, 'Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)' (2007) COM/2007/0228 final

——, 'Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive' (2007) COM/2007/0087 final

——, 'Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification (Notified under Document Number C(2009) 3200)' (2009) 2009/387/EC

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' (2010) COM(2010)609

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards Interoperability for European Public Services' (2010) COM/2010/0744 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century' (2012) COM/2012/09 final

——, 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data' (2012) COM/2012/010 final-2012/0010 (COD)

——, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' (2012) COM/2012/011 final-2012/0011 (COD)

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Thriving Data-Driven Economy' (2014) COM/2014/0442 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building A European Data Economy' (2017) COM (2017) 9 final

——, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2017) COM(2017) 10 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a Common European Data Space.' (2018) COM(2018) 232 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe' (2018) COM(2018) 237 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' (2020) COM(2020) 66 final

——, 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust' (2020) COM(2020) 65 final

——, 'Communication from the Commission to the European Parliament and the Council. Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' (2020) COM/2020/264 final

——, 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2020) COM/2020/767 final.

——, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (2020) COM/2020/825 final

——, 'Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' (2020) COM/2020/842 final

——, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Fostering a European Approach to Artificial Intelligence' (2021) COM(2021) 205 final

——, 'Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2021) COM(2021) 206 final

——, 'Proposal for a Regulation Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (2021) COM(2021) 206 final

——, 'Special Eurobarometer 487a – March 2019 "The General Data Protection Regulation" Report (2019) <https://data.europa.eu/doi/10.2838/579882> accessed 8 June 2021

European Commission, Directorate-General for Justice and Consumers, and TNS Opinion & Social, Special Eurobarometer 431 "Data Protection" Report (2015) <http://dx.publications.europa.eu/10.2838/552336> accessed 8 June 2021

European Commission's High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Scientific Disciplines' (European Commission's High-Level Expert Group on Artificial Intelligence 2019)

——, 'Ethics Guidelines for Trustworthy AI.' (European Commission - Directorate General for Communications Networks, Content and Technology 2019)

European Parliament, 'European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence' (2020) P9_TA(2020)0276

——, 'European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on the Digital Services Act: Improving the Functioning of the Single Market' (2020) P9_TA(2020)0272

European Parliament. Committee on Civil Liberties, Justice and Home Affairs (LIBE), 'Opinion on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (2021) PE692.898v07

European Parliament. Directorate General for Parliamentary Research Services., A Governance Framework for Algorithmic Accountability and Transparency. (Publications Office 2019)

EDPS, EDPB and WP29 acts

Article 29 Data Protection Working Party, 'Opinion 10/2004 on More Harmonised Information Provisions' (25 November 2004) WP 100

——, 'Opinion 4/2007 on the Concept of Personal Data' (20 June 2007) WP 136

——, 'Opinion 2/2010 on Online Behavioural Advertising' (22 June 2010) WP 171

——, 'Opinion 15/2011 on the Definition of Consent' (13 July 2011) WP187

——, 'Opinion 1/2012 on the Data Protection Reform Proposal' (23 March 2012) WP 191

——, 'Opinion 3/2013 on Purpose Limitation' (2 April 2013) WP203

——, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (16 September 2014) WP 223

——, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (30 May 2014) WP218

——, 'Guidelines on Data Protection Officers ('DPOs')' (13 December 2016) WP243rev.01

——, 'Guidelines on the Lead Supervisory Authority' (13 December 2016) wp244rev.01

——, '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) WP248rev.01

——, 'Guidelines on the Right to "Data Portability"' (5 April 2017) WP242rev.01

——, 'Guidelines on Transparency under Regulation 2016/679' (29 November 2017) WP260 rev.01

——, 'Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)' (4 October 2017) WP 252

——, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (6 February 2018) WP251rev.01

——, 'Guidelines on Consent under Regulation 2016/679' (8 April 2018) WP259rev.01

Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (1 December 2009) WP 168

European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020)

——, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020)

——, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR' (7 July 2020)

——, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (7 September 2020)

——, 'Individual Replies from the Data Protection Supervisory Authorities' (2020) <https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en>

——, 'Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications' (9 March 2021)

——, 'Guidelines 8/2020 on the Targeting of Social Media Users' (13 April 2021)

——, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' (5 August 2021)

——, 'Statement on the Digital Services Package and Data Strategy' (18 November 2021)

European Data Protection Board - European Data Protection Supervisor, 'Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities' (12 March 2019)

——, 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (11 March 2021)

European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy' (18 March 2010)

——, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A Comprehensive Approach on Personal Data Protection in the European Union"' (14 January 2011)

——, 'Opinion of the European Data Protection Supervisor on the Data Protection Reform Package' (7 March 2012)

——, 'Opinion on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems' (8 June 2012)

——, 'Opinion 7/2015 Meeting the Challenges of Big Data.' (19 November 2015)

——, 'Opinion 9/2016 EDPS Opinion on Personal Information Management Systems' (20 October 2016)

——, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (14 March 2017)

——, 'Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (EPrivacy Regulation)' (24 April 2017)

——, 'Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies' (16 March 2018)

——, 'Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data' (19 March 2019)

——, 'Opinion 1/2021 on the Proposal for a Digital Services Act' (10 February 2021)

——, 'EDPS Inspection Software' <https://edps.europa.eu/edps-inspection-software_en> accessed 1 November 2021

European Data Protection Supervisor - European Data Protection Board, 'Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (18 June 2021)

——, 'GDPR: A Three-Year-Old Who Must Still Learn to Walk before It Runs | European Data Protection Supervisor' <https://edps.europa.eu/press-publications/press-news/blog/gdpr-three-year-old-who-must-still-learn-walk-it-runs_en>

CJEU case law

Case C-28/08P Commission v Bavarian Lager [2010]

Case C-25/17, Jehovan todistajat [2018] ECLI:EU:C:2018:551

Case C-40/17, Fashion ID [2019] ECLI:EU:C:2019:629

Case C-61/19, Orange Romania [2020] ECLI:EU:C:2020:901

Case C-70/10, Scarlet Extended [2011] ECLI:EU:C:2011:771

Case C-73/07, Satakunnan Markkinapörssi e Satamedia [2008] ECLI:EU:C:2008:727

Case C-92/09, Volker und Markus Schecke e Eifert [2010] ECLI:EU:C:2010:662

Case C-101/01, Lindqvist [2003] ECLI:EU:C:2003:596

Case C-131/12, Google Spain e Google [2014] ECLI:EU:C:2014:317

Case C-141/12, YS e a [2014] ECLI:EU:C:2014:2081

Case C-201/14, Bara e a [2015] ECLI:EU:C:2015:638

Case C-230/14, Weltimmo [2015] ECLI:EU:C:2015:639

Case C-275/06, Promusicae [2008] ECLI:EU:C:2008:54

Case C-291/12, Schwarz [2013] ECLI:EU:C:2013:670

Case C-293/12, Digital Rights Ireland [2014] ECLI:EU:C:2014:238

Case C-311/18, Facebook Ireland e Schrems [2020] ECLI:EU:C:2020:559

Case C-345/17, Buivids [2019] ECLI:EU:C:2019:122

Case C-362/14, Schrems [2015] ECLI:EU:C:2015:650

Case C-434/16, Nowak [2017] ECLI:EU:C:2017:994

Case C-461/10, Bonnier Audio e a [2012] ECLI:EU:C:2012:219

Case C-465/00, Österreichischer Rundfunk e a [2003] ECLI:EU:C:2003:294

Case C-507/17, Google (Territorial scope of de-referencing) [2019] ECLI:EU:C:2019:772

Case C-543/09, Deutsche Telekom [2011] ECLI:EU:C:2011:279

Case C-553/07, Rijkeboer [2009] ECLI:EU:C:2009:293

Case C-582/14, Breyer [2016] ECLI:EU:C:2016:779

Case C-615/13 P, ClientEarth and PAN Europe v EFSA [2010] ECLI:EU:C:2015:489

Case C-673/17, Planet49 [2019] ECLI:EU:C:2019:801

Other materials

Access Now, 'Three Years under the EU GDPR' (Access Now 2021) <https://www.accessnow.org/gdpr-three-years/>

——, 'How to Fix the EU Artificial Intelligence Act' (Access Now, 7 September 2021) <https://www.accessnow.org/how-to-fix-eu-artificial-intelligence-act/> accessed 17 November 2021

Acquisti A and others, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50 ACM Computing Surveys 1

——, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50 ACM Computing Surveys 1

Acquisti A, Brandimarte L and Loewenstein G, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509 <https://www.science.org/doi/10.1126/science.aaa1465> accessed 20 November 2021

Acquisti A and Grossklags J, 'Privacy and Rationality' in Katherine J Strandburg and Daniela Stan Raicu (eds), Privacy and Technologies of Identity (Springer-Verlag 2006)

Ada Lovelace Institute - UK AI Council, 'Exploring Legal Mechanisms for Data Stewardship - Chapter 1 Data Trusts' (Ada Lovelace Institute - UK AI Council 2021) <https://www.adalovelaceinstitute.org/feature/data-trusts/#fnref-6>

——, 'Exploring Legal Mechanisms for Data Stewardship - Chapter 2 Data Cooperatives' (Ada Lovelace Institute - UK AI Council 2021) <https://www.adalovelaceinstitute.org/feature/data-trusts/#fnref-6>

AGCOM, AGCM, Garante per la protezione dei dati personali, 'Indagine Conoscitiva Sui Big Data (Annex 1 Resolution n. 458/19/CONS)' (2019)

Alemanno A, 'Nudging Smokers The Behavioural Turn of Tobacco Risk Regulation' (2012) 3 European Journal of Risk Regulation 32

Algorithmic Watch, Open Knowledge Foundation Deutschland, 'OpenSCHUFA' (OpenSchufa) <https://openschufa.de/english/> accessed 2 November 2021

AlgorithmWatch, 'AlgorithmWatch's Response to the European Commission's Proposed Regulation on Artificial Intelligence – A Major Step with Major Gaps' (AlgorithmWatch) <https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/> accessed 17 November 2021

Allen AL, Unpopular Privacy: What Must We Hide? (Oxford University Press 2011)

Alvisi C, 'I trattamenti nel settore bancario, finanziario e assicurativo' in Licia Califano and Carlo Colapietro (eds), Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679 (Editoriale scientifica 2017)

'An Update on Facebook's Human Rights Work in Asia and Around the World' (Meta, 12 May 2020) <https://about.fb.com/news/2020/05/human-rights-work-in-asia/> accessed 17 November 2021

Anciaux N and others, 'Personal Data Management Systems: The Security and Functionality Standpoint' (2019) 80 Information Systems 13

Anrig B, Browne W and Gasson M, 'The Role of Algorithms in Profiling' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen (Springer Netherlands 2008) <http://link.springer.com/10.1007/978-1-4020-6914-7_4> accessed 7 July 2021

App Drivers and Courier Unions, 'Collective Action Campaign to Claim Your Data from Uber' <https://www.adcu.org.uk/wie> accessed 2 November 2021

Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymisation of Large Datasets. (How to Break Anonymity of Netflix Prize Dataset)' [2008] Proceedings - IEEE Symposium on Security and Privacy 111

Asghari H, van Biemen T and Warnier M, 'Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests' [2021] arXiv:2106.06844 [cs]

——, 'Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests' [2021] Proceedings of the The 5th Workshop on Technology and

Consumer Protection (ConPro'21), IEEE, 2021. <http://arxiv.org/abs/2106.06844> accessed 2 November 2021

Ausloos J and Dewitte P, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4

Ausloos J and Veale M, 'Researching with Data Rights' [2021] Technology and Regulation 136

Ballell TR de las H and others, 'Work Stream on Data: Final Report' (European Commission 2021)

Baloup J and others, 'White Paper on the Data Governance Act' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3872703> accessed 15 December 2021

Barocas S and Nissenbaum H, 'Big Data's End Run around Anonymity and Consent' in Helen Nissenbaum and others (eds), Privacy, Big Data, and the Public Good: Frameworks for Engagement (Cambridge University Press 2014)

Bauer JM, Bergstrøm R and Foss-Madsen R, 'Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data' (2021) 120 Computers in Human Behavior 106729

Beauchamp TL and Childress JF, Principles of Biomedical Ethics (5th ed, Oxford University Press 2001)

Bellavista A, 'Art. 17' in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), La tutela dei dati personali: commentario alla L. 675-1996 (2. ed, CEDAM 1999)

Bennett CJ, 'Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s' (1991) 16 Science, Technology, & Human Values 51

——, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press 1992)

Ben-Shahar O and Chilton A, 'Simplification of Privacy Disclosures: An Experimental Test' (2016) 45 The Journal of Legal Studies S41

Bergemann B, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen and others (eds), Privacy and Identity Management. The Smart Revolution (Cham: Springer International Publishing 2018)

Bernardi S, 'Commento All'art. 17: Trattamento Che Presenta Rischi Specifici' in C Massimo Bianca and Francesco Donato Busnelli (eds), La protezione dei dati personali: commentario al D. lgs. 30 giugno 2003, n. 196: codice della privacy (CEDAM 2007)

Beyer M and Laney D, 'Report: The Importance of Big Data: A Definition' (Gartner Analysis 2012)

Bhageshpur K, 'Council Post: Data Is The New Oil -- And That's A Good Thing' Forbes (15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/> accessed 14 June 2021

Bieker F, 'Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice' in Anja Lehmann and others (eds), Privacy and Identity Management. Facing up to Next Steps, vol 498 (Springer International Publishing 2016)

Binns R, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22

Bloustein EJ, Individual and Group Privacy (Transaction Books 1978)

Bohannon J, 'Credit Card Study Blows Holes in Anonymity' (2015) 347 Science 468

Bollier D, 'The Promise and Perils of Big Data' (Aspen Institute 2010)

Borgeswius FZ, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 IEEE Security & Privacy 103

Bostrom N, Superintelligence: Paths, Dangers, Strategies (First edition, Oxford University Press 2014)

Braga A and Logan R, 'The Emperor of Strong AI Has No Clothes: Limits to Artificial Intelligence' (2017) 8 Information 156

Brandimarte L, Acquisti A and Loewenstein G, 'Misplaced Confidences: Privacy and the Control Paradox' (2013) 4 Social Psychological and Personality Science 340

Brave, 'New Data on GDPR Enforcement Agencies Reveal Why the GDPR Is Failing' (Brave 2020) <https://brave.com/dpa-report-2020/> accessed 1 November 2021

Bravo F, 'L'«architettura» Del Trattamento e La Sicurezza Dei Dati e Dei Sistemi' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (G Giappichelli editore 2019)

——, 'Le Condizioni Di Liceità Del Trattamento Di Dati Personali' in Giusella Finocchiaro (ed), La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101 (Prima edizione, Zanichelli editore 2019)

Brkan M, 'Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond' [2017] SSRN Electronic Journal

——, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91

Bruns A, 'After the "APIcalypse": Social Media Platforms and Their Fight against Critical Scholarly Research' (2019) 22 Information, Communication & Society 1544

Burkert H, 'Privacy-Enhancing Technologies: Typology, Critique, Vision' in Philip E Agre and Marc Rotenberg (eds), Technology and privacy: the new landscape (MIT Press, Cambridge, MA, USA 1997)

Buttarelli G, Banche Dati e Tutela Della Riservatezza: La Privacy Nella Società Dell'informazione: Commento Analitico Alle Leggi 31 Dicembre 1996, Nn. 675 e 676 in Materia Di Trattamento Dei Dati Personali e Alla Normativa Comunitaria Ed Internazionale (Giuffrè 1997)

Bygrave LA, 'AUTOMATED PROFILING' (2001) 17 Computer Law & Security Review 17

Bygrave LA, Data Protection Law: Approaching Its Rationale, Logic, and Limits (Kluwer Law International 2002)

Bygrave LA and Schartum DW, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Netherlands 2009)

Cadwalladr C, 'Follow the Data: Does a Legal Document Link Brexit Campaigns to US Billionaire?' The Observer (14 May 2017) <https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns> accessed 22 December 2021

——, 'UK Regulator Orders Cambridge Analytica to Release Data on US Voter' The Guardian (5 May 2018) <https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-uk-regulator-release-data-us-voter-david-carroll> accessed 2 November 2021

Caggia F, 'Libertà Ed Espressione Del Consenso' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (G Giappichelli editore 2019)

Caggiano IA, 'Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo(GDPR) e analisi comportamentale. Iniziali spunti di riflessione' [2017] Diritto Mercato Tecnologia <https://www.dimt.it/la-rivista/articoli/il-consenso-al-trattamento-dei-dati-personali-tra-nuovo-regolamento-europeo-gdpr-e-analisi-comportamentale-iniziali-spunti-di-riflessione/> accessed 19 December 2021

Califano L, 'Il Ruolo Di Vigilanza Del Garante per La Protezione Dei Dati Personali' (2020) 33 federalismi.it

Calo R, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2012) 87 Notre Dame Law Review 1051

Camera dei deputati, Banche Dati e Tutela Della Persona (1981)

Canhoto A and Backhouse J, 'General Description of the Process of Behavioural Profiling' in Serge Gutwirth and Mireille Hildebrandt (eds), Profiling the European Citizen (Springer Netherlands 2008)

Cardarelli F, 'Cooperazione, assistenza e operazioni' in Roberto D'Orazio and others (eds), Codice della privacy e data protection (Giuffrè Francis Lefebvre 2021)

——, 'Indipendenza e autorità di controllo' in Roberto D'Orazio and others (eds), Codice della privacy e data protection (Giuffrè Francis Lefebvre 2021)

Caridi V, 'Sub Art. 15' in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), La tutela dei dati personali: commentario alla L. 675-1996 (2. ed, CEDAM 1999)

Carolan E, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32 Computer Law & Security Review 462

Cate FH, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), Consumer protection in the age of the 'information economy' (Ashgate 2006)

Cate FH and Mayer-Schönberger V, 'Notice and Consent in a World of Big Data' (2013) 3 International Data Privacy Law 67

Cavoukian A, Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-Makers and Policy-Makers (Information and Privacy Commissioner of Ontario, Canada 2011)

——, Privacy by Design. From Rethoric to Reality (Information and Privacy Commissioner of Ontario, Canada 2014)

——, 'Privacy by Design. The 7 Foundational Principles.' Information and Privacy Commissioner of Ontario

Clark S, 'Exclusive: Strained Irish Data Regulator Gets Big Staff Boost' Global Data Review (7 May 2021) <https://globaldatareview.com/data-privacy/exclusive-strained-irish-data-regulator-gets-big-staff-boost> accessed 1 November 2021

Clarke R, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer Law & Security Review 123

Council of Europe, Legislation and Data Protection: Proceedings of the Rome Conference on Problems Relating to the Development and Application of Legislation on Data Protection (Camera dei Deputati 1983)

Cuijpers C, 'A Private Law Approach to Privacy; Mandatory Law Obliged?' (2007) 4 SCRIPT-ed 304

Custers B, van der Hof S and Schermer B, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users' (2014) 6 Policy & Internet 268 <http://doi.wiley.com/10.1002/1944-2866.POI366> accessed 8 June 2021

D'Acquisto G and others, Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics. (European Network and Information Security Agency 2015)

D'Acquisto G, Naldi M and D' Acquisto G (eds), 'Anonimizzazione', Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza (Giappichelli 2017)

D'Anastasio C and Mehrotra D, 'The Creators Of Pokémon Go Mapped The World. Now They're Mapping You' (Kotaku) <https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714> accessed 11 January 2022

Daigle B and Khan M, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' [2020] Journal of International Commerce and Economics <https://www.usitc.gov/journals>

De Hert P, 'Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism' in Stefano Montaldo, Francesco Costamagna and Alberto Miglio (eds), EU Law Enforcement The Evolution of Sanctioning Powers (Routledge 2021)

——, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), Privacy and the criminal law (Intersentia 2006)

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Netherlands 2009)

De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179

De Montjoye Y-A and others, 'Predicting Personality Using Novel Mobile Phone-Based Metrics' in Ariel M Greenberg, William G Kennedy and Nathan D Bos (eds), Social Computing, Behavioral-Cultural Modeling and Prediction, vol 7812 (Springer Berlin Heidelberg 2013)

De Montjoye Y-A and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536

De Montjoye, Y-A, Schweitzer H and Crémer J, Competition Policy for the Digital Era. (European Commission 2019)

De Witte B, 'The Past and Future Role of the European Court of Justice in the Protection of Human Rights' in Philip Alston, Mara R Bustelo and James Heenan (eds), The EU and human rights (Oxford University Press 1999)

Deakins S, 'Data Is The New Water: Seven Reasons Why' HuffPost UK (12 October 2017) <https://www.huffingtonpost.co.uk/stjohn-deakins-/data-is-the-new-water-sev_b_18228184.html> accessed 14 June 2021

Debusseré F, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?' (2005) 13 International Journal of Law and Information Technology 70

Delacroix S and Lawrence ND, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' [2019] International Data Privacy Law ipz014

Dell'Utri M, 'Principi Generali e Condizioni Di Liceità Del Trattamento Dei Dati Personali' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (G Giappichelli editore 2019)

Di Genio G, 'Trasparenza e accesso ai dati personali' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), La nuova disciplina europea della 'privacy' (Wolters Kluwer 2016)

Dille G, 'Sen. Wyden to Reintroduce AI Bias Bill in Coming Months' (19 February 2021) <https://www.meritalk.com/articles/sen-wyden-to-reintroduce-ai-bias-bill-in-coming-months/> accessed 17 November 2021

Dimitrova A and Brkan M, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair: Balancing National Security and Data Protection' (2018) 56 JCMS: Journal of Common Market Studies 751

D'Orazio R, in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), La tutela dei dati personali: commentario alla L. 675-1996 (2. ed, CEDAM 1999)

——, 'Protezione dei dati by default e by design' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), La nuova disciplina europea della privacy (Wolters Kluwer 2016)

Ducato R and others, 'Legal Design Manifest' <https://www.legaldesignalliance.org/>

Duportail J, 'I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets' The Guardian (26 September 2017) <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold> accessed 2 November 2021

Dworkin G, 'Paternalism' (The Stanford Encyclopedia of Philosophy, Fall Edition 2020) <https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=paternalism> accessed 17 December 2021

ECP | Platform voor de InformatieSamenleving, 'Artificial Intelligence Impact Assessment' (ECP | Platform voor de InformatieSamenleving 2018) <https://ecp.nl/publicatie/artificial-intelligence-impact-assessment-english-version/> accessed 17 November 2021

Edwards L and Veale M, '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

Egan E, 'Data Portability and Privacy' (Facebook 2019)

Electronic Privacy Information Center (EPIC), 'Feedback from: The Electronic Privacy Information Center (EPIC)' (6 August 2021) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665484_en> accessed 17 November 2021

European Digital Rights (EDRi), 'Open Letter: EDRi Urges Enforcement and Actions for the 2 Year Anniversary of the GDPR' (edri.org) <https://edri.org/our-work/open-letter-edri-urges-enforcement-and-actions-for-the-2-year-anniversary-of-the-gdpr/> accessed 2 November 2021

European Union Agency for Fundamental Rights, Strengthening the Fundamental Rights Architecture in the EU.II, Data Protection in the European Union : The Role of National Data Protection Authorities. (Publications Office 2010)

'Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections' (Meta, 9 April 2018) <https://about.fb.com/news/2018/04/new-elections-initiative/> accessed 1 November 2021

Ferraris V and others, 'Defining Profiling' [2013] Woking Paper 1 of the EU Project "Profiling - Protecting Citizens' Rights Fighting Illicit Profiling" <available at: http://www.ssrn.com/abstract=2366564> accessed 2 December 2021

Finocchiaro G, 'Il Diritto All'oblio Nel Quadro Dei Diritti Della Personalità.' in Giorgio Resta and Vincenzo Zeno-Zencovich (eds), Il diritto all'oblio su Internet dopo la sentenza Google Spain (RomaTrePress 2015)

——, 'La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems' (2015) 31 Diritto dell'informazione e dell'informatica 779

——, 'Il Quadro d'insieme Sul Regolamento Europeo Sulla Protezione Dei Dati Personali' in Giusella Finocchiaro (ed), La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101 (Prima edizione, Zanichelli editore 2019)

——, 'Intelligenza Artificiale e Diritto - Intelligenza Artificiale e Protezione Dei Dati Personali' (2019) 7 Giurisprudenza Italiana 1657

Fiona Carlin, 'The Data Protection Directive: The Introduction of Common Privacy Standards' (1996) 21 European Law Review 65

Flaherty D, 'Privacy Impact Assessments: An Essential Tool for Data Protection' (2000) 7 Privacy Law and Policy Reporter 85

Flaherty DH, Privacy and Government Data Banks: An International Perspective (Mansell 1979)

——, 'Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies' (1986) 11 Science, Technology, & Human Values 7

——, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (University of North Carolina Press 1989)

Floridi L, 'Group Privacy: A Defence and an Interpretation' in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Foxe K, 'Data Protection Commission "Acutely Strained" by Big Tech Cases' (The Irish Times) <https://www.irishtimes.com/business/technology/data-protection-commission-acutely-strained-by-big-tech-cases-1.4457683> accessed 1 November 2021

Freese J, 'The Swedish Data Act' (1977) 178 Current Sweden

Fried C, 'Privacy' (1968) 77 Yale Law Journal 475

Froomkin AM, 'Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements' (2015) 2015 University of Illinois Law Review 1713

Fuster GG and Gellert R, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology 73

Future of Privacy Forum, 'The Privacy Expert Guide To Artificial Intelligence and Machine Learning' (Future of Privacy Forum 2018)

Gallus GB, in Ettore Giannantonio, Mario G Losano and Vincenzo Zeno-Zencovich (eds), La tutela dei dati personali: commentario alla L. 675-1996 (2. ed, CEDAM 1999)

Garante per la protezione dei dati personali, 'HACKtheDOC: il primo hackathon italiano di legal design. Il Garante per la protezione dei dati personali propone la challenge "Infoprivacy"' (2020) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9500152> accessed 18 December 2021

——, 'Semplificare Le Informative Privacy Attraverso Il Metodo "Creative Commons". Protocollo Tra Garante Privacy e Creative Commons' (2021) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9684797> accessed 18 December 2021

Gatt L, Montanari R and Caggiano IA, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 48 Politica del diritto 363

Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421

Gellert R, van Bekkum M and Borgesius FZ, 'The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making' [2021] Eu Law Analysis blog <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html> accessed 7 July 2021

German Federal Government's Data Ethics Commission, 'Opinion of the Data Ethics Commission' (23 October 2019) <https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html>

Giannone Codiglione G, 'Risk-based approach e trattamento dei dati personali' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), La nuova disciplina europea della 'privacy' (Wolters Kluwer 2016)

Giovannella F, 'Le Persone e Le Cose: La Tutela Dei Dati Personali Nell'ambito Dell'Internet of Things' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (Giappichelli 2019)

Giurgiu A and Larsen T, 'Roles and Powers of National Data Protection Authorities' (2016) 2 European Data Protection Law Review <https://orbilu.uni.lu/handle/10993/29819> accessed 29 October 2021

Glennon M and others, The European Data Market Monitoring Tool. Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories. D2.9 Final Study Report. (European Commission 2020)

Gonçalves ME, 'The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective' (2020) 23 Journal of Risk Research 139

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

Goodman B and Flaxman S, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 AI Magazine 50

'Google's Human Rights by Design' (BSR, 30 October 2019) <https://www.bsr.org/en/our-insights/blog-view/google-human-rights-impact-assessment-celebrity-recognition> accessed 17 November 2021

Götzmann N and others, 'Huma Rights Impact Assessment - Guidance and Toolbox' (The Danish Institute for Human Rights 2016)

Graef I, Husovec M and Purtova N, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359

Guardigli E, 'Le Autorità Di Controllo: Dalla Direttiva 95/46/CE al Regolamento n. 679/2016' in Giusella Finocchiaro (ed), La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101 (Prima edizione, Zanichelli editore 2019)

Guidotti R and others, 'A Survey of Methods for Explaining Black Box Models' (2019) 51 ACM Computing Surveys 1

Haapio H and others, 'Legal Design Patterns for Privacy' in Erich Schweighofer and others (eds), Data protection/LegalTech: proceedings of the 21st International Legal Informatics Symposium (Editions Weblaw 2018)

Hagen M, Law by Design (2018) <https://lawbydesign.co/>

——, Legal Design (2018) <https://lawbydesign.co/>

Haile T, 'What You Think You Know About the Web Is Wrong' (Time, 9 March 2014) <https://time.com/12933/what-you-think-you-know-about-the-web-is-wrong/> accessed 8 June 2021

Hansen M, Jensen M and Hoepman J-H, Readiness Analysis for the Adoption and Avolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan : Approved, Version 1.0, Public. (European Network and Information Security Agency 2015)

Hansen PG, 'The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?' (2016) 7 European Journal of Risk Regulation 155

Harrison J and Stephenson M-A, 'Human Rights Impact Assessment : Review of Practice & Guidance for Future Assessments.' (Scottish Human Rights Commission 2010)

Hartzog W, 'The Case Against Idealising Control' (2018) 4 European Data Protection Law Review 423

Hern A, 'Cambridge Analytica: How Did It Turn Clicks into Votes?' The Guardian (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 15 October 2021

Hijmans H, 'The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?' (2016) 2 European Data Protection Law Review 362

——, The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016)

——, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?' (2018) 4 European Data Protection Law Review 80

Hildebrandt M, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen (Springer Netherlands 2008)

——, 'Who Is Profiling Who? Invisible Visibility' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Netherlands 2009)

——, 'The Dawn of a Critical Transparency Right for the Profiling Era', Digital Enlightenment Yearbook (IOS Press 2012)

Hodgson C, 'Facebook given Deadline to Share Data for Research' Financial Times (28 August 2019) <https://www.ft.com/content/147eddec-c916-11e9-af46-b09e8bfe60c0> accessed 1 November 2021

Hondius FW, Emerging Data Protection in Europe (North-Holland Pub Co ; American Elsevier Pub Co 1975)

Hoofnagle C and others, 'How Different Are Young Adults From Older Adults When It Comes to Information Privacy Attitudes & Policies?' [2010] Departmental Papers (ASC) <https://repository.upenn.edu/asc_papers/523>

Hull G, 'Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data' (2015) 17 Ethics and Information Technology 89

Hurley M and Adebayo J, 'Credit Scoring in the Era of Big Data' (2017) 18 Yale Journal of Law and Technology <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5>

Hustinx P, 'The Role of Data Protection Authorities' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Netherlands 2009)

——, 'Privacy by Design: Delivering the Promises' (2010) 3 Identity in the Information Society 253

——, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' <https://edps.europa.e/ite/d/ile/ublicatio/4-09-15_article_eui_en.pdf>

IDC Infobrief, sponsored by Qlik, 'Data as the New Water: The Importance of Investing in Data and Analytics Pipelines' (2020)

Information Commissioner's Office (ICO), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection v. 2.2' (2017)

——, 'Nudge Techniques' (14 October 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/> accessed 18 December 2021

International Association for Impact Assessment, 'What Is Impact Assessment?' (International Association for Impact Assessment 2009) <https://www.iaia.org/reference-and-guidance-documents.php>

Ioannou A and others, 'Privacy Nudges for Disclosure of Personal Information: A Systematic Literature Review and Meta-Analysis' (2021) 16 PLOS ONE <https://dx.plos.org/10.1371/journal.pone.0256822> accessed 18 December 2021

Jacob VM, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 The Yale Journal 513

*Jang W and Newman AL, 'Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation *' [2021] JCMS: Journal of Common Market Studies jcms.13215*

Janger EJ, 'Privacy Property, Information Costs, and the Anticommons' (2003) 54 Hastings L. J. 899

Janssen H and others, 'Decentralized Data Processing: Personal Data Stores and the GDPR' (2021) 10 International Data Privacy Law 356

Jaquet-Chiffelle D-O, 'Reply: Direct and Indirect Profiling in the Light of Virtual Persons' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen (Springer Netherlands 2008)

John McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' 27 AI Magazine 12

Jòri A, 'Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities' (2015) 5 International Data Privacy Law 133

Kamarinou D, Millard C and Hon WK, 'Cloud Privacy: An Empirical Study of 20 Cloud Providers' Terms and Privacy Policies—Part I: Table A1' (2016) 6 International Data Privacy Law 79

Kaminski ME and Malgieri G, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2021) 11 International Data Privacy Law 125

Kammourieh L and et. al, 'Group Privacy in the Age of Big Data' in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Kang J and Buchner B, 'Privacy in Atlantis' (2004) 18 Harvard Journal of Law & Technology. 230

Kelion L, 'Amazon's Ring Logs Every Doorbell Press and App Action' BBC News (4 March 2020) <https://www.bbc.com/news/technology-51709247> accessed 2 November 2021

Kirby M, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 International Data Privacy Law 6

Kirby MD, 'Transborder Data Flows and the Basic Rules of Data Privacy' (1980) 16 Stanford Journal of International Law 27

——, 'The OECD Privacy Guidelines @ 30. Remarks to the OECD Working Party for Information Security and Privacy' (Paris, 9 March 2010)

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250

Kosinski M, Stillwell D and Graepel T, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110 Proceedings of the National Academy of Sciences 5802 <http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110>

Kosta E, Consent in European Data Protection Law (Martinus Nijhoff Publishers 2013)

Krämer J, Senellart P and Streel A de, 'Making Data Portability More Effective for the Digital Economy' (Centre on Regulation in Europe, CERRE 2020)

Kreimer S, 'The Freedom of Information Act and the Ecology of Transparency' (2008) 10 University of Pennsylvania Journal of Constitutional Law 1011

Kröger JL, Lutz OH-M and Ullrich S, 'The Myth of Individual Control: Mapping the Limitations of Privacy Self-Management' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3881776>

Kroll J and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633

Kumm M, 'Internationale Handelsgesellschaft, Nold and the New Human Rights Paradigm' in Miguel Poiares Maduro and Loïc Azoulai (eds), The past and future of EU law: the classics of EU law revisited on the 50th anniversary of the Rome Treaty (Hart 2010)

La Quadrature du Net, 'First Sanction against Google Following Our Collective Complaints' (laquadrature.net, 21 January 2019) <https://www.laquadrature.net/en/2019/01/21/first-sanction-against-google-following-our-collective-complaints/> accessed 2 November 2021

Laney D, '3D Data Management: Controlling Data Volume, Velocity, and Variety | BibSonomy' (META Group 2001) <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>

Larsen R and others, 'Report on Personal Data Stores' (European Commission 2015)

Latonero M, 'Governing Artificial Intelligence' (Data & Society, 10 October 2018) <https://datasociety.net/library/governing-artificial-intelligence/> accessed 17 November 2021

Lazaro C and Le Métayer D, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12 SCRIPTed <http://script-ed.org/?p=1927> accessed 7 June 2021

Leiser MR and Dechesne F, 'Governing Machine-Learning Models: Challenging the Personal Data Presumption' (2020) 10 International Data Privacy Law 187

Lessig L, 'Reading The Constitution in Cyberspace' [1997] SSRN Electronic Journal <http://www.ssrn.com/abstract=41681> accessed 10 June 2021

——, Code and Other Laws of Cyberspace (Basic Books 1999)

——, 'Privacy as Property' (2002) 69 Social Research: An International Quarterly 247

Libelium, 'Report: 50 Sensor Applications for a Smarter World', (9 September 2020)' (Libelium 2020) <https://www.libelium.com/libeliumworld/top_50_iot_sensor_applications_ranking/>

Lindblad Kernell E, Bloch Veiberg C and Jacquot C, 'Guidance on Human Rights Impact Assessment of Digital Activities' (The Danish Institute for Human Rights 2020)

Lindqvist J, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) 26 International Journal of Law and Information Technology 45

Loi M and others, 'Automated Decision-Making Systems in the Public Sector – An Impact Assessment Tool for Public Authorities' (Algorithmic Watch 2021)

Lynch M, 'Data Wars: Unlocking the Information Goldmine - BBC News' BBC News (13 April 2012) <https://www.bbc.com/news/business-17682304> accessed 14 June 2021

Lynskey O, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569

——, The Foundations of EU Data Protection Law (First edition, Oxford University Press 2015)

——, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 European Law Review 793

Macario F, 'La Protezione Dei Dati Personali Nel Diritto Privato' in Vincenzo Cuffaro and Vincenzo Ricciuto (eds), La disciplina del trattamento dei dati personali (G Giappichelli 1997)

Mahieu R and Ausloos J, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' (LawArXiv 2020) preprint

Mahieu RLP, Asghari H and van Eeten M, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review

Malgieri G, 'Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data' (2016) 4 Privacy in Germany 133

——, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review

Malgieri G and Comandé G, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243

Mantelero A, 'The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law & Security Review 643

——, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 Computer Law & Security Review 238

——, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

——, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law & Security Review 584

——, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754

——, 'La Gestione Del Rischio' in Giusella Finocchiaro (ed), La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101 (Prima edizione, Zanichelli editore 2019)

——, 'La Privacy All'epoca Dei Big Data' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (Giappichelli 2019)

——, 'Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies' (Council of Europe 2019)

——, 'Valutazione d'impatto sulla protezione dei dati' in Roberto D'Orazio and others (eds), Codice della privacy e data protection (Giuffrè Francis Lefebvre 2021)

Mantelero A and Esposito MS, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 105561

Manyika J and others, 'Big Data: The next Frontier for Innovation, Competition, and Productivity | McKinsey' (McKinsey Global Institute 2011) <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation> accessed 7 July 2021

Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Philip E Agre and Marc Rotenberg (eds), Technology and Privacy: The New Landscape (The MIT Press 1997)

Mayer-Schönberger V and Cukier K, Big Data: A Revolution That Will Transform How We Live, Work and Think (Murray 2013)

Mazzamuto S, 'Il Principio Del Consenso e Il Potere Della Revoca' in Rocco Panetta (ed), Libera circolazione e protezione dei dati personali (Giuffrè 2006)

McCubbins MD and Schwartz T, 'Congressional Oversight Overlooked: Police Patrols versus Fire Alarms' (1984) 28 American Journal of Political Science 165

McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4 J. L. & POL'Y FOR INFO. SOC'Y 543

Mefford A, 'Lex Informatica: Foundations of Law on the Internet' (1997) 5 Indiana Journal of Global Legal Studies 211

Mendoza I and Bygrave LA, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), EU Internet Law (Springer International Publishing 2017)

Merchant RM and others, 'Evaluating the Predictability of Medical Conditions from Social Media Posts' (2019) 14 PLOS ONE e0215476

Michael Veale, 'Netflix Claim They Only Use Individual Choices to Inform Which Video Segments to Show, Although They Do Learn from Aggregate Choices, as Would Be Expected' (12 February 2019) <https://twitter.com/mikarv/status/1095110950028562433>

Micheli M and others, 'Emerging Models of Data Governance in the Age of Datafication' (2020) 7 Big Data & Society 205395172094808

Miller AR, The Assault on Privacy: Computers, Data Banks, and Dossiers (Univ of Michigan Press 1971)

Miller K, 'Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data' (Stanford HAI) <https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data> accessed 15 December 2021

Moerel L and Prins C, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' [2016] SSRN Electronic Journal <http://www.ssrn.com/abstract=2784123>

Moor JH, 'Towards a Theory of Privacy in the Information Age' (1997) 27 ACM SIGCAS Computers and Society 27

Moss E and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' (Data&Society 2021)

Mühlhoff R, 'Predictive Privacy: Towards an Applied Ethics of Data Analytics' [2021] Ethics and Information Technology <https://link.springer.com/10.1007/s10676-021-09606-x>

Ng A, 'We Need to Talk about Default Settings for Privacy' (CNET, 21 December 2019) <https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/> accessed 18 December 2021

Nissenbaum H, 'Toward an Approach to Privacy in Public: Challenges of Information Technology' (1997) 7 Ethics & Behavior 207

NOYB, 'Netflix, Spotify & YouTube: Eight Strategic Complaints Filed on "Right to Access"' (noyb.eu) <https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access> accessed 1 November 2021

——, 'Noyb Files 422 Formal GDPR Complaints on Nerve-Wrecking "Cookie Banners"' (noyb.eu) <https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners> accessed 2 November 2021

OECD, 'The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines', vol 176 (OECD 2011) OECD Digital Economy Papers 176

——, 'OECD Digital Economy Papers: The Internet of Things: Seizing the Benefits and Addressing the Challenges', vol 252 (OECD 2016) OECD Digital Economy Papers 252

O'hara K, Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship (University of Southampton 2019)

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA L. Rev. 1701

Open Data Institute, 'Defining a "Data Trust"' (Open Data Institute 2018) <https://theodi.org/article/defining-a-data-trust/> accessed 9 November 2021

Open Rights Group, 'Who Do Political Parties Think We Are?' (action.openrightsgroup.org) <https://action.openrightsgroup.org/who-do-political-parties-think-we-are-4> accessed 2 November 2021

Ordemann H-J and Schomerus R, Bundesdatenschutzgesetz: BDSG (5. Aufl, Beck 1992)

Pagallo U, '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? (Springer Netherlands 2012)

——, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Luciano Floridi, Linnet Taylor and Bart Van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Pagano R, Panorama of Personal Data Protection Laws (Camera dei Deputati 1983)

Panoptykon Foundation, 'Panoptykon Files Complaints against Google and IAB Europe' (panoptykon.org, 28 January 2019) <https://en.panoptykon.org/complaints-Google-IAB> accessed 2 November 2021

Paracampo MT, 'FinTech Tra Algoritmi, Trasparenza e Algo-Governanc' (2019) 2 Diritto della banca e del mercato finanziario 213

Pardolesi R and Palmieri A, 'Il Codice in Materia Di Protezione Dei Dati Personali e l'intangibilità Della "Privacy" Comunitaria' (2004) IV Foro italiano 59

Parent WA, 'Privacy, Morality, and the Law' (1983) 12 Philosophy & Public Affairs 269

Pasquale F, The Black Box Society: The Secret Algorithms That Control Money and Information (First Harvard University Press paperback edition, Harvard University Press 2016)

Peppet SR, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 87

Perez AJ, Zeadally S and Cochran J, 'A Review and an Empirical Analysis of Privacy Policy and Notices for Consumer Internet of Things' (2018) 1 Security and Privacy

Peters B, 'The Big Data Gold Rush' New York: Forbes Magazine (21 June 2012) <https://www.forbes.com/sites/bradpeters/2012/06/21/the-big-data-gold-rush/> accessed 14 June 2021

Piccone V and Pollicino O (eds), La Carta dei diritti fondamentali dell'Unione europea: efficacia ed effettività (Editoriale scientifica 2018)

Pizzetti F, Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo (Seconda ristampa, G Giappichelli 2016)

Pollicino O, 'Interpretazione o Manipolazione? La Corte Di Giustizia Definisce Un Nuovo Diritto Alla Privacy Digitale' (2014) 3 federalismi.it - focus TMT <https://www.federalismi.it/nv14/articolo-documento.cfm?artid=28017>

——, 'Un Digital Right to Privacy Preso (Troppo) Sul Serio Dai Giudici Di Lussemburgo? Il Ruolo Degli Artt. 7 e 8 Della Carta Di Nizza Nel Reasoning Di Google Spain' in Giorgio Resta and Vincenzo Zeno-Zencovich (eds), Il diritto all'oblio su Internet dopo la sentenza Google Spain (RomaTrePress 2015)

—— (eds), Constitutional Challenges in the Algorithmic Society (1st edn, Cambridge University Press 2021)

Pollicino O and Bassini M, 'La Carta Dei Diritti Fondamentali Dell'Unione Europea Nel Reasoning Dei Giudici Di Lussemburgo' (2015) 4/5 Il diritto dell'informazione e dell'informatica 741

——, 'Sub Art. 8' in Roberto Mastroianni and others (eds), Carta dei diritti fondamentali dell'Unione europea (Giuffrè editore 2017)

——, 'La Cassazione Sul "Consenso Algoritmico". Ancora Un Tassello Nella Costruzione Di Uno Statuto Giuridico Composito' [2021] Giustizia Insieme <https://www.giustiziainsieme.it/it/news/127-main/diritto-e-innovazione/1800-la-cassazione-sul-consenso-algoritmico-ancora-un-tassello-nella-costruzione-di-uno-statuto-giuridico-composito> accessed 7 July 2021

Prins C, 'Property and Privacy: European Perspectives and the Commodification of Our Identity' (2006) 15 Information Law Series 223

Privacy International, 'What Does Twitter Know about Its Users? #NOLOGS' (privacyinternational.org, 16 February 2012) <http://privacyinternational.org/blog/1504/what-does-twitter-know-about-its-users-nologs> accessed 2 November 2021

——, 'Data Is Power: Profiling and Automated Decision-Making in GDPR' (2018) <https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr>

——, 'Tell Companies to Stop Exploiting Your Data! | Privacy International' (privacyinternational.org, 8 November 2018) <https://privacyinternational.org/campaigns/take-control-your-data> accessed 2 November 2021

Purtova N, Property Rights in Personal Data: A European Perspective (Kluwer Law International 2012)

——, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (2017) 10 Journal of Law and Economic Regulation 64

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

Quelle C, 'Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann and others (eds), Privacy and Identity Management. Facing up to Next Steps, vol 498 (Springer International Publishing 2016)

Raab C and Szekely I, 'Data Protection Authorities and Information Technology' (2017) 33 Computer Law & Security Review 421

Raab C and Wright D, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul de Hert (eds), Privacy impact assessment (Springer 2012)

Raab CD, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 105404

Rachels J, 'Why Privacy Is Important' (1975) 4 Philosophy & Public Affairs 323

Reddix-Smalls B, 'Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market' (2011) 12 UC Davis Business Law Journal 87

Reding V, 'The Upcoming Data Protection Reform for the European Union' (2011) 1 International Data Privacy Law 3

——, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2 International Data Privacy Law 119

Regan PM, Legislating Privacy: Technology, Social Values and Public Policy (The Univ of North Carolina Press 2009)

Reidenberg JR, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 911

——, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 553

Reisman D and others, 'Algorithmic Impact Assessment: A Pracical Framework for Public Agency Accountability' (AI Now 2018)

René Arnold, Annette Hillebrand, and Martin Waldburger, 'Personal Data and Privacy Final Report, Studi for Ofcom' (WIK-Consult 2015)

Resta G, 'The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives' (2011) 26 Tulane European and Civil Law Forum 33

Riccardi JL, 'The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?' (1983) 6 Boston College International and Comparative Law Review 243

Ricci A, 'I Diritti Dell'interessato' in Giusella Finocchiaro (ed), La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs.10 agosto 2018, n. 101 (Prima edizione, Zanichelli editore 2019)

Riccio GM and others, 'The POSEID-ON Blockchain-Based Platform Meets the "Right to Be Forgotten"' (2020) 2 Rivista di diritto dei media 194

Ricciuto V, 'La Patrimonializzazione Dei Dati Personali. Contratto e Mercato Nella Ricostruzione Del Fenomeno' in Vincenzo Cuffaro, Roberto D'Orazio and Vincenzo Ricciuto (eds), I dati personali nel diritto europeo (2019)

Richmond B, 'A Day in the Life of Data: Removing the Opacity Surrounding the Data Collection, Sharing and Use Environment in Australia' (Consumer Policy Research Centre 2019) Report

Rodotà S, Elaboratori Elettronici e Controllo Sociale (Il Mulino 1973)

——, Tecnologie e Diritti (Il Mulino 1995)

——, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Netherlands 2009)

Rodrigues R, 'David Wright, Trilateral Ltd. - Ethical Impact Assessment Will Make R&I More Responsible!' <https://satoriproject.eu/publications/trilateral-david-wright/> accessed 16 November 2021

Roig A, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8 European Journal of Law and Technology

Roppo V, 'I Diritti Della Personalità' in Guido Alpa and Mario Bessone (eds), Banche dati, telematica e diritti della persona (CEDAM 1984)

Rosenblat A, Kneese T and Boyd D, 'Networked Employment Discrimination' (Data & Society 2014) Future of Work Project supported by Open Society Foundations <https://www.datasociety.net/pubs/fow/EmploymentDiscrimination.pdf>

Rossi A and others, 'When Design Met Law: Design Patterns for Information Transparency' [2019] Droit de la Consommation

Rossi A and Palmirani M, 'Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection' (2020) 36 Design Issues 82

Rouvroy A, '"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data' (Bureau Of The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data 2015) Ets 108

Rouvroy A and Poullet Y, '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? (Springer Netherlands 2009)

Royal Society (Great Britain), Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis. (2019)

Rubinstein IS, 'Regulating Privacy by Design' (2011) 26 Berkeley Technology Law Journal 1409

Rubinstein IS, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74

Ruhaak A, 'Data Trusts: Why, What and How' [2019] Algorithmic Watch <https://algorithmwatch.org/en/data-trusts-why-what-and-how/>

——, 'When One Affects Many: The Case For Collective Consent' [2020] Mozilla Foundation <https://foundation.mozilla.org/en/blog/when-one-affects-many-case-collective-consent/> accessed 9 November 2021

Samuelson P, 'Privacy As Intellectual Property?' (2000) 52 Stanford Law Review 1125

Sartor G, 'Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz"' (1986) XII Informatica e diritto 95

——, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (an Parliamentary Research Service 2020)

Sartor G and De Azevedo Cunha MV, 'Il Caso Google e i Rapporti Regolatori Usa/EU' (2014) 4/5 Diritto dell'informazione e dell'informatica 657 ss

Sartor G, Lagioia F and Galli F, 'Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent' (European Parliament's Committee on Legal Affairs 2021)

Satariano A, 'Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates - The New York Times' The New York Times (27 April 2020) <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html> accessed 1 November 2021

SATORI Project, 'Ethical Assessment of Research and Innovation: A Comparative Analysis of Practices and Institutions in the EU and Selected Other Countries' (SATORI Project 2016) Deliverable D1.1 <https://satoriproject.eu/work_packages/comparative-analysis-of-ethics-assessment-practices/>

——, 'A Common Framework for Ethical Impact Assessment - Annex 1' (SATORI Project 2016) Deliverable D4.1 <https://satoriproject.eu/work_packages/roadmap-for-a-common-eu-ethics-assessment-framework/>

Scally D, 'Irish Data Regulator Sparks Row with EU Colleagues on Facebook Oversight' (The Irish Times) <https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065> accessed 1 November 2021

Scaria E and others, Study on Data Sharing between Companies in Europe: Final Report. (European Commission 2018)

Schwartz P and Reidenberg JR, 'Commissioned Study: Online Services and Data Protection and Privacy. Regulatory Response' (European Commission 1998)

Schwartz PM, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 8 Iowa Law Review 471

——, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices' [2000] Wisconsin Law Review

——, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056

Scrinis G and Parker C, 'Front-of-Pack Food Labeling and the Politics of Nutritional Nudges: Front-of-Pack Food Labeling' (2016) 38 Law & Policy 234

Secretariat TB of C, 'Algorithmic Impact Assessment Tool' (22 March 2021) <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> accessed 17 November 2021

Selbst AD, 'Disparate Impact in Big Data Policing' (2017) 52 Georgia Law Review 109

Selbst AD and Powles J, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233

Shoemaker DW, 'Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity' (2010) 12 Ethics and Information Technology 3

Siano M, 'Il diritto all'oblio in Europa e il recente caso spagnolo' in Franco Pizzetti (ed), Il caso del diritto all'oblio (G Giappichelli 2013)

Sica S and D'Antonio V, 'La Procedura Di De-Indicizzazione' 2014 Diritto dell'informazione e dell'informatica 703

Sica S, Stanzione P and Riccio GM, 'Sub Art. 33', La nuova disciplina della privacy: commento al D. lgs. 30 giugno 2003, n. 196 (Zanichelli 2005)

Simitis S, 'Zwanzig Jahre Datenschutz in Hessen - Eine Kritische Bilanz' (1990) 19 Tatigkeitsbericht des Hessischen Datenschutzbeauftragten 138

——, 'Einleitung: Geschichte—Ziele—Prinzipien' in Spiros Simitis and others (eds), Bundesdatenschutzgesetz (Nomos-Verl-Ges 2011)

Sinha A, 'A Case for Greater Privacy Paternalism? — The Centre for Internet and Society' The Center for Internet & Society (14 February 2016) <https://cis-india.org/internet-governance/blog/a-case-for-greater-privacy-paternalism#_ftnref16> accessed 1 December 2021

Solove DJ, Understanding Privacy (Harvard University Press 2009)

——, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880

——, 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds), Social Dimensions of Privacy (Cambridge University Press 2015) <https://www.cambridge.org/core/product/identifier/9781107280557%23CN-bp-4/type/book_part> accessed 7 June 2021

Spaventa E, 'Fundamental Rights in EU Law' in Catherine Barnard and Steve Peers (eds), European union law (Oxford University Press 2017)

Stone Sweet A, 'The European Court of Justice and the Judicialization of EU Governance' (2010) 5 Living Reviews in European Governance <http://europeangovernance-livingreviews.org/Articles/lreg-2010-2/> accessed 19 June 2021

Sundar SS and others, 'Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key?', CHI '13 Extended Abstracts on Human Factors in Computing Systems (Association for Computing Machinery 2013)

Sunstein CR and Thaler RH, 'Libertarian Paternalism Is Not an Oxymoron' (2003) 70 The University of Chicago Law Review 1159 <https://www.jstor.org/stable/1600573> accessed 17 December 2021

Supergovernance, 'A Canadian Algorithmic Impact Assessment' (Medium, 18 March 2018) <https://medium.com/@supergovernance/a-canadian-algorithmic-impact-assessment-128a2b2e7f85> accessed 17 November 2021

——, 'The Government of Canada's Algorithmic Impact Assessment: Take Two' (Medium, 8 August 2018) <https://medium.com/@supergovernance/the-government-of-canadas-algorithmic-impact-assessment-take-two-8a22a87acf6f> accessed 17 November 2021

Tait J, 'The Case for Data Cooperatives' (The Data Economy Lab 2021) <https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives/> accessed 15 December 2021

Tavani HT, 'Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy' (2007) 38 Metaphilosophy 1

Tavani HT and Moor JH, 'Privacy Protection, Control of Information, and Privacy-Enhancing Technologies' (2001) 31 ACM SIGCAS Computers and Society 6

Temme M, 'Algorithms and Transparency in View of the New General Data Protection Regulation' (2017) 3 European Data Protection Law Review 473

Tene O and Polotensky J, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 1 Nw. J. Tech. & Intell. Prop. 239

Thaler RH and Sunstein CR, Nudge: Improving Decisions about Health, Wealth, and Happiness (Rev and expanded ed, Penguin Books 2009)

'The Importance of the Ethical and Privacy Impact Assessment Plus in the INGENIOUS Project' (Trilateral Research, 7 December 2020) <https://www.trilateralresearch.com/the-importance-of-the-ethical-and-privacy-impact-assessment-plus-in-the-ingenious-project/> accessed 16 November 2021

Torino R, 'La valutazione d'impatto (Data Protection Impact Assessment)' in Salvatore Sica, Virgilio D'Antonio and Giovanni Maria Riccio (eds), La nuova disciplina europea della 'privacy' (Wolters Kluwer 2016)

Tzanou M, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88

Urquhart L, Lodge T and Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1

Vale SB, Zanfir-Fortuna G and Van Eijk R, 'Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022' (Future of Privacy Forum 2021)

Van Alsenoy B, Kosta E and Dumortier J, 'Privacy Notices versus Informational Self-Determination: Minding the Gap' (2014) 28 International Review of Law, Computers & Technology 185

van der Sloot B, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307

van Erp SJHM, 'From "classical" to Modern European Property Law' in Konstantinos D Kerameus (ed), Essays in honour of Konstantinos D. Kerameus (Ant N Sakkoulas ; Bruylant 2009)

Van Geuns J and Brandusescu A, 'What Does It Mean? | Shifting Power Through Data Governance' (Mozilla Foundation 2020) <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/> accessed 9 November 2021

Veale M, Binns R and Edwards L, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180083

'Vestager on the Intersection of Data and Competition' IAPP (30 October 2018) <https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/> accessed 5 July 2021

Voigt P and Von Dem Bussche A, The EU General Data Protection Regulation (GDPR) (Springer Berlin Heidelberg 2017)

Wachter S, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10 Law, Innovation and Technology 266

Wachter S, Mittelstadt B and Floridi L, '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

Wachter S, Mittelstadt B and Russell C, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

Weiser M, 'The Computer for the 21st Century' (1991) 265 Scientific American 94

Westin A, 'Privacy And Freedom' (1968) 25 Washington and Lee Law Review 166 <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>

Westin AF, Privacy and Freedom (Atheneum 1967)

'What's the PESIA Framework? – VIRT-EU' (virt.eu, 30 October 2018) <https://blogit.itu.dk/virteuproject/2018/10/30/whats-the-pesia-framework/> accessed 16 November 2021

Wiewiórowski W, 'Civil Society Organisations as Natural Allies of the Data Protection Authorities | European Data Protection Supervisor' (15 May 2018) <https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_de>

Wong J and Henderson T, 'The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR' (2019) 9 International Data Privacy Law 173

Worker Info Exchange, 'Data Rights for Digital Workers' (workerinfoexchange.org) <https://www.workerinfoexchange.org> accessed 2 November 2021

——, 'Gig Workers Score Historic Digital Rights Victory against Uber & Ola' (workerinfoexchange.org) <https://www.workerinfoexchange.org/post/gig-workers-score-historic-digital-rights-victory-against-uber-ola-2> accessed 2 November 2021

Wright D, 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13 Ethics and Information Technology 199

——, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307

Wright D, Finn R and Rodrigues R, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries' (2013) 9 Journal of Contemporary European Research 160

Wright D and Friedewald M, 'Integrating Privacy and Ethical Impact Assessments' (2013) 40 Science and Public Policy 755

Wright D and Hert P de (eds), Privacy Impact Assessment (Springer 2012)

Wright D and Raab CD, 'Constructing a Surveillance Impact Assessment' (2012) 28 Computer Law & Security Review 613

Youyou W, Kosinski M and Stillwell D, 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans' (2015) 112 Proceedings of the National Academy of Sciences 1036

Ziegeldorf JH, Morchon OG and Wehrle K, 'Privacy in the Internet of Things: Threats and Challenges: Privacy in the Internet of Things: Threats and Challenges' (2014) 7 Security and Communication Networks 2728

Zuboff S, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (First edition, PublicAffairs 2019)

Zuiderveen Borgesius FJ, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 The International Journal of Human Rights 1572