LUISS

Corso di laurea in Giurisprudenza

Cattedra EU Substantive Law: Internal Market and Beyond

The free movement of data in Europe: GDPR, balancing data protection with the better functioning of the Internal Market

Prof. Daniele Gallo

RELATORE

Prof. Giacomo Biagioni

CORRELATORE

Matr. 155 413 Gabriele Cattaneo

CANDIDATO

Anno Accademico 2022/2023

Table of Contents

INTRODUCTION

In today's digitally interconnected world, the handling and protection of personal data have become central concerns not only for individuals but also for governments, businesses, and organizations. At the heart of this global conversation lies the General Data Protection Regulation (GDPR), a comprehensive framework enacted by the European Union (EU) to govern the processing and transfer of personal data. As data breaches and privacy violations increasingly make headlines, the GDPR represents a landmark attempt to safeguard the rights and privacy of individuals while addressing the challenges posed by the digital age.

The right to privacy, considered a fundamental – yet not absolute – human right in the EU, finds explicit recognition in various legal charters and conventions other from the and the European Charter of Fundamental Rights, including the Universal Declaration of Human Rights and the European Convention on Human Rights. In the context of the EU, nonetheless, this right takes on additional significance due to the Union's unique commitment to preserving and advancing individual rights within its borders. Reflecting the historical progression of Member States' traditions concerning freedom and the right to the secrecy of correspondence, the EU possesses a longstanding tradition of privacy rights that has evolved since its inception. The Treaties establishing the European Communities, which laid the foundation for the modern EU, demonstrated an early recognition of the importance of protecting personal data, even before the digital era transformed the data landscape. This commitment has continually evolved through subsequent treaties and legal instruments, ultimately culminating in the incorporation of data protection laws, of which GDPR stands as a cornerstone.

In this thesis, we argue that to fully grasp the implications of the GDPR in the EU data protection framework and to better appreciate its outcomes, it becomes essential to navigate the complexities that define its scope. Notwithstanding its name, the General Data Protection Regulation, as a regulatory framework, is more than a set of rules governing data. It showcases a complex structure of legal provisions and principles carefully crafted to balance the rights of individuals with the needs of the digital age. At its core, the GDPR aims to protect the fundamental right to privacy while fostering the free flow of data, a delicate equilibrium that resonates not only within the European Union but also reverberates on the global stage.

The two aims at first glance might appear (and arguably are) at odds: for instance, rapid advancements in technology – such as the recent upsurge in Artificial Intelligence and big data analytics – require extensive data processing rending the balancing of data protection with these technological innovations a truly complex task. Nonetheless, in today's data-driven landscape, achieving a good balance between the two interests might be the cornerstone on which to build a conscious yet thriving society, making the effort from the European legislator all the more comprehensible.

In arguing that the acknowledgement of this multifaceted interplay between data protection, individual rights and broader economic and technological contexts is relevant for comprehending the GDPR's global influence as well, this research will embark on a thorough examination of the Regulation. Commencing by retracing the steps that led to its ultimate implementation, in the opening chapter, we embark on an analysis of the legal and historical main events which influenced how the Regulation is crafted today, delving into the legal foundations of data protection within the European Union (EU) all the way to the pioneering work of the Council of Europe which helped shaping the data protection framework we have today.

Our analytical journey extends to an exploration of influential pre-GDPR legal cases, dissecting their implications and contributions to the broader data protection landscape. This analytical approach equips us with a comprehension of the intricate legal terrain that preceded the GDPR's enactment.

By engaging in this analysis of historical events and legal precedents, we cultivate a comprehensive understanding of the historical roots which preceded data protection laws. Our objective is to present a well-founded narrative rooted in factual events and legal developments, providing the foundation for a deeper examination of the Regulation's impact and significance.

As we venture deeper into the analysis, our focus shifts to its core principles and objectives. Chapter II explores how the Regulation adeptly navigates the complex terrain between safeguarding data privacy and fostering the free movement of data within the EU. Stemming from a recognition of data as an increasingly valuable asset, we dissect the GDPR's structure and its foundational principles, alongside other important pieces of legislation which go to complete nowadays' legal digital landscape. Our examination unravels the intricate interplay between privacy and the free flow of data, revealing the

Regulation's role as a catalyst in the overall strategy of the EU to obtain growth in research, technological innovation and economy.

Chapter III propels us beyond the EU's borders to assess the global impact of the GDPR. Five years since its implementation, we delve into the Regulation's profound influence on data protection practices worldwide. We explore the emergence of the "GDPR model", the possible reasons behind what has been a global phenomenon and its far-reaching effects. Furthermore, through case studies and real-world applications, we scrutinize the GDPR's adaptability in the ever-evolving technological landscape.

All in all, this thesis embarks on a comprehensive journey through the multifaceted understanding of the GDPR. From its historical foundations to its global impact, interactions with emerging technologies, and practical enforcement, our ultimate objective is to critically evaluate whether the GDPR effectively accomplishes its dual mission: safeguarding personal data while facilitating the free movement of this data—a challenging endeavor which risks not to fully satisfy either goal.

CHAPTER I - GDPR IN THE MAKING, TRACKING THE PATH TOWARD THE REGULATION

1. The Legislative Path towards the GDPR

European data law is a legal domain that includes, but goes beyond, data protection law, which is the well-known area of law concerned with the protection of personal data and, by extension, individual privacy[1]. This legal domain bears a rich historical foundation, stretching back in time and characterized by a lineage of key contributors, each playing a significant role in its evolution over time. The path that led toward the General Data Protection Regulation[2] was indeed driven by a combination of technological advancements, changing societal norms, and the need to address the complexities of data protection in an increasingly digital world. Early initiatives in data protection originating from (now Members) States, the ECHR and the EU – along with said challenges posed by technological advancements[3] – all played significant roles in shaping the Regulation.

Therefore, the focus of this first chapter will be given to the historical and legal path that resulted in the adoption of the GDPR, delving into the specific key events and currents prior its entry into force. Understanding this background is crucial for comprehending the intent and scope of the GDPR, how and – most of all – why it deals with data protection issues the way it does, as well as its impact on data protection practices and privacy rights within the EU and beyond.

Thomas Streinz, in tracing the origins of European Data Protection law, rightfully points out how "before there was European data protection law, there was data protection law in Europe[4]" willing to emphasize how important the contributions stemming from single

[1] Thomas Streinz, *'The Evolution of European Data Law'*, in Paul Craig, and Gráinne de Búrca (eds), The Evolution of EU Law, 3rd edn (2021) at 902; as the author also recognizes, the relationship between 'data protection' and 'privacy' is complicated and contested. Yet, this thesis will focus on EU law, without ignoring the Council of Europe's significant contributions.
[2] 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) from now on "GDPR" or "the Regulation"; ECLI:EU:C:2014:317
[3] Supra Thomas Streinz, at 905.
[4] Ibid, at 904.

States in the early 70's has been for the regulatory framework we have today. It is also important to stress, however, that before that, the groundwork for a right to privacy can be traced back to the legal protections afforded from said States to the freedom and secrecy of correspondence. Almost all European constitutions encompass a broader Right to Communications Confidentiality[5], extending the traditional protections of secrecy in correspondence to include electronic communications [6]

These legal protections initially offered within individual Member States for freedom and secrecy of correspondence served as a foundation that was later recognized and amplified within a series of international agreements[7]. As we delve further into the subject, we will explore the distinct achievements of both the Council of Europe and the European Union.

For several decades, in fact, the two European regional institutions have both taken legislative action on privacy and data protection. Nevertheless, the texts adopted on both sides have unavoidable links demonstrating the two institutions' reciprocal influence[8].

2. European Convention of Human Rights and the build up from Article 8

The Council of Europe, founded in 1949, established the European Convention on Human Rights[9] in 1950 with the aim of safeguarding human rights and freedoms in Europe. Amongst these rights, Article 8 guarantees individuals a right to respect for their "private

[5] See Belgium 1831 Constitution. Art. 22; Netherlands 1814 (rev. 2008) Constitution Art. 13 (Neth.); Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 28 June 2022, Art. 10; Costituzione della Repubblica Italiana Art. 15. For more on communications confidentiality in national constitutions, see Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič, '*A Typology of Privacy'*, University of Pennsylvania Journal of International Law 483 (2017).

[6] For an in-depth analysis of the Right to Communications Confidentiality, see Frederik J. Zuiderveen Borgesius, Wilfred Steenbruggen, '*The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust*', Theoretical Inquiries in Law, Forthcoming, (2018).

[7] *Inter alia*, Art. 8 of the European Convintion on Human Rights, art. 7 of the Charter of Fundamental Rights of the European Union, art. 17 of the International Covenant on Civil and Political Rights, art. 11 of the American Convention on Human Rights

[8] Cécile de Terwangne, '*Council of Europe convention 108+: A modernised international treaty for the protection of personal data'*, Computer Law & Security Review, Volume 40, (2021), at 2.

[9] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950.

and family life, his home, and his correspondence"[10]. These rights are not unrestricted; rather, they are "in accordance with the law" and "necessary in a democratic society" and are therefore not absolute."

Yet, the right to data protection was conspicuously lacking from the European Convention on Human Rights and it would not have been recognized until much later.

The necessity for more organized and precise regulations to protect people's personal data became gradually more evident in the years after the European Convention on Human Rights was adopted as well as the need for a comprehensive treaty on the protection of individuals' personal data, which was thus started. With electronic computers first beginning to gather and process personal data in the late 1960s, concerns about the consequences of computer-based record-keeping vigorously began to surface in Europe for the first time.

Another step forward was taken by the "Younger Committee" group based in the UK, which conducted in the 1970's a thorough investigation of the issue and came to the conclusion that the current remedies, particularly privacy remedies under common law, were insufficient to handle this new threat. Their Report (the "Younger Committee Report on Privacy"[11]) already highlighted data processing principles that are now at the heart of current EU data protection law.

Even before the publication of the Younger Report, some Member States had already adopted the view that a new category of legislation was necessary to address the dangers posed by the automated processing of personal data. On October 7th, 1970, the German state of Hesse passed the first law[12] in history aimed exclusively at regulating automated data processing in the public sector. Several other German states did the same, while in Sweden a task group was established to investigate the issues that computerized record keeping could bring about as there was intense opposition in 1969 to the collection of census data in a way that would assist automated data processing.

In fact, the *trait d'union* theme of these earliest responses to computer-based record keeping in Europe was indeed the acknowledgement that automated data processing exposes people to risks that the (at the time) existing legal framework – including privacy laws – was unable to appropriately address. This alleged regulatory gap would have been filled by data protection laws: its guiding principle is that automated processing of personal data must be

[10] *Ibid*, art. 8.
[11] Gerald Dworkin, '*The Younger Committee Report on Privacy'*, 1973; The Modern Law Review, 36(4), 399–406,
[12] Hessisches Datenschutzgesetz [1970] GVBl I 625.

fair, and its underlying premise is that, unless it complies with the data management standards required by data protection law, automated processing negatively affects people which is why, as opposed to privacy law, exercising rights granted under data protection law does not require proof of harm[13]. The initial common idea, therefore, was that processing – that is automated – causes harm.

2.1 The "beta" of GDPR, Convention 108

In response to the aforementioned concerns, other significant contributions from the CoE that would have had far-reaching implications for the future are found in the Council's initial interventions in the area by releasing a resolution in 1973 on the protection of people from private sector electronic data processing banks[14]. This was followed by another resolution in 1974 that was unique to public sector data banks, with both resolutions promoting fairness in the processing.

Being resolutions non-binding, the CoE worked towards the creation of a binding treaty that would have come to life with the CoE's most important achievement in data protection, this being the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[15] (Convention 108). The Convention 108, signed on 28 January 1981 in Strasbourg (nowadays known as Data Protection Day) represents the first legal instrument adopted at the European level on the protection of personal data, as well as the only legally binding international treaty on the subject.

The adoption of the Convention resulted from the Council of Europe Member States' recognition that article 8 of the ECHR ("Right to Respect for Private and Family life") could not provide adequate protection for individual rights in the context of personal data processing on its own[16]. In this regard, Convention 108 represents one of the main stages in

[13] Golden Data Law, '*The History of Data protection Law*,' Medium (2018), available at https://medium.com/golden-data/data-protection-law-how-it-all-got-started-df9b82ef555e

[14] Council of Europe, Committee of ministers, resolution (73)*22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*, (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies).

[15] Convention *for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28.I.1981. Adhering Members at the moment: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherland, North Macedonia, Norway, Poland, Portgual, Republic of Moldova, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkiye, Ukraine, United Kingdom. Treaty open for signature by the Member States and for accession by non-Member States.

[16] See '*Italy signs the Protocol amending the Convention 108'*, Cyberlaws, by ICT Legal Consulting, (2019) available at https://www.cyberlaws.it/2019/italy-signs-the-protocol-amending-the-convention-108/.

the emancipation of personal data protection from the right to respect for private life enshrined in the ECHR.

In our analysis, the study of the Convention gets all the more important on account of the fact that, in recognizing the need for transparency in data processing practices and the necessity of obtaining informed consent from data subjects, it served as a foundation for all subsequent data protection legislation. Convention 108 already highlighted the crucial role of independent supervisory authorities in ensuring the enforcement of data protection laws: these authorities were tasked with monitoring compliance, investigating complaints, and imposing sanctions in cases of non-compliance with the establishment of such authorities being aimed at providing individuals with accessible ways to address concerns related to the processing of their personal data.

Transnational data flows were a further topic covered by Convention 108. Prior to it, several EU Member States restricted data transfers to other Members on account of the fact that privacy standards varied across European countries. The treaty established the fundamental principle that signatory nations "shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.[17]" Furthermore, transfers may only be restricted in cases where the importing jurisdiction does not offer "equivalent protection" where a signatory country has particular legislation protecting personal data. Even today's EU cross-border data transfer regulations are based on this 1981 regulation, with the European Data Protection Board issuing new guidelines periodically which follow this purposes[18].

Convention 108 had a profound influence on the development of national data protection laws across Europe. Members of the Council of Europe were obliged to incorporate the provisions of Convention 108 into their respective legal systems, thereby promoting (even if with some tangible differences and still at a surface level) a quasi-harmonized approach to data protection within the region, notwithstanding that the principles and framework outlined in the Convention served as a reference for countries when formulating their own data protection legislation. Member States sought to align their laws with the convention's requirements, ensuring a surface level of consistency and coherence in data protection practices.

[17] *Ibid*, Art. 12.
[18] For the last in chronological order, see Guidelines 05/2021 *on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Adopted on 14 February 2023.

Convention 108 also played a pivotal role in initiating ongoing discussions and developments in the field of data protection as it laid the foundation for subsequent international agreements and initiatives aimed at strengthening data protection worldwide as the principles and concepts introduced by Convention 108 continue to resonate in contemporary data protection laws (concepts such as informed consent, purpose limitation, and the establishment of supervisory authorities remain central to modern data protection frameworks). The legacy of Convention 108 can be observed in subsequent legal instruments, including the EU Data Protection Directive[19] and finally echoing in the GDPR, both of which built upon and expanded the principles set forth by the Convention[20].

2.2 The EU Data Protection Directive (1995)

While Convention 108 laid the groundwork for international standards on data protection it was not tailored to the unique needs and legal complexities of the European Community. The national legislations adopted by European States in the late 1970s and early 1980s contained too many disparities, which hampered the development of the European common market[21]. Consequently, the EU passed Directive 95/46[22] in an attempt to further harmonize the data protection regimes of EU Member States[23], with the Directive unequivocally stating that it intended to build and expand on the principles outlined in the CoE's Convention 108[24].

The Convention establishes general principles, while the EU texts (Directive 95/46 and GDPR) specifics a detailed legal regime for data protection[25].

---

[19] Bruno Gencarelli, former head of the European Commission's data protection unit in the Justice Department, mantained "*Convention 108 is not only a piece of paper, it is a living document and it provides for a standard setting process on a very wide range of issues. Even the EU's data protection directive for law enforcement is inspired partly by Convention 108*.".

[20] Wrangu, 'What is Convention 108?', Blog, 2018 available at https://www.wrangu.com/what-is-convention-108/.

[21] See Recitals 7 and 8 directive 95/46/EC.

[22] Directive 95/46/EC 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*, 24 October 1995; ECLI:EU:C:2015:650

[23] *Ibid* Recital 8.

[24] *Ibid,* Recital 11 recites: "Whereas 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 am- plify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Auto- matic Processing of Personal Data".

[25] *Supra* Cécile de Terwangne, '*Council of Europe convention 108+: A modernised international treaty for the protection of personal data',* at 2.

In Italy, the directive was implemented through Legislative Decree No. 196 of 30 June 2003[26], known as the Personal Data Protection Code. The decree integrated the provisions of the EU directive, along with several other national laws relating to data protection, into a consolidated legal framework.

Structured in a Preamble and eight chapters, raging from general rules for the lawfulness of the processing activity to the wider discipline of transfer of data to third countries, the contribution of the Directive was significant as it introduced numerous key principles which are now at the very core of the GDPR. Among others[27], it is worth underlying the requirement for data controllers to process personal data fairly and lawfully, to specify the purpose of data collection and use enshrined in Article 6. Article 7, on the other hand, requires for the processing of data the unambiguous consent from the subject, consent on which the GDPR will place the focus of its entire discipline.

Further essential contributions set by the Directive included: Article 12, which provided individuals with a right to access information regarding the processing of their personal data; Article 16, enabling the right to rectification, erasure, or blocking of incorrect data; and Article 25, which set forth principles relating to the transfer of data to third countries, stipulating that data could only be transferred if an "adequate level of protection" was ensured.

While the directive was an important step, it still allowed for some flexibility in implementation, as it required each Member State to enact its national laws to comply with the directive's requirements. Inconsistencies in its implementation across Member States highlighted the need for a more uniformed legal framework and underscored the significance of moving from a directive to a singular, overarching regulation with direct applicability. It is important to distinguish between a directive and a regulation. The first establishes a set of general guidelines, but only becomes enforceable when Member States incorporate it into national law. Regulations, on the other hand, already have binding legal force[28]. As a result, GDPR applies to all Member States without the need for national legislation, thereby

[26] Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali", in S.O n. 123 alla G.U. 29 luglio 2003, n. 174.
[27] For an in-depth analysis of the changes and elements that have remained constant from the Data Protection Directive to GDPR, see Christopher Kuner, Lee A Bygrave, Christopher Docksey, '*Background and Evolution of the EU General Data Protection Regulation (GDPR)*', in Christopher Kuner and others (eds), Chapter in 'The EU General Data Protection Regulation (GDPR): A Commentary*'* , Oxford Academic (2020), 1 – 47.
[28] Junwoo Seo Kyoungmin Kim, Mookyu Park, Moosung Park and Kyungho Lee, "*An analysis of economic impact on IoT under GDPR*", 8th International Conference on ICT Convergence (ICTC), (2018), at 879..

unifying European Union rules and laws[29]. Such a transition also aimed to circumvent the disparities by ensuring a standardized approach to data protection across the entire European Union as the rapid advancement of digital technologies (and the proliferation of online services) completely transformed the data landscape.

Nonetheless, the EU Data Protection Directive still laid the foundation for a comprehensive and harmonized approach to data protection within the EU. In providing a framework for Member States to develop their own national data protection laws – aligning them with the directive's principles – the Directive set the stage for the subsequent adoption of the General Data Protection Regulation (GDPR), which aimed to address the shortcomings of the directive and introduce more robust data protection standards.

2.3 Other milestones leading to the GDPR

2.3.1. Lisbon Treaty (2007)

Another landmark development in data protection law was the Treaty of Lisbon of 2007. The entry into force of the Lisbon Treaty in 2009 gave the Charter[30] the same legal value as the Treaties and abolished the pillar structure providing a stronger basis for a more effective and comprehensive EU data protection regime and emphasizing the need for a coherent data protection framework. The first pillar, which used the Community method to protect data for private and commercial purposes, and the third pillar, which used the intergovernmental level to protect data for law enforcement purposes, made up the legislation governing data protection in the area of freedom, security, and justice (AFSJ).

In the second pillar, nevertheless, there was no general legal framework on data protection. This lack would stem from the fact that the common foreign and security policy was established as a space for intergovernmental cooperation, where legal instruments are more likely to address broad strategies and actions aimed at maintaining peace and bolstering international security than they are to address particular individuals[31]. As a result, the rules

[29] Freitas and Mira da Silva, "*GDPR compliance in SMEs: there is much to be done", Journal of Information Systems Engineering & Management,* Vol. 34 No. 4, (2018) at 30.

[30], Art. 8 of the Charter deals with the protection of personal data and is articulated as follows: "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".

[31] Hielke Hijmans and Alfonso Scirocco, '*Shortcomings in EU Data Protection in the third and the second pillars. Can the Lisbon treaty be expected to help*?', (2009); Common Market Law Review, 46, at 1497.

for making decisions in each area were different. The pillar structure disappeared with the Lisbon Treaty, which provides a stronger basis for development and a more effective data protection system EU introducing a provision specifically targeting data protection (Art. 16 TFEU[32]) with general application, which means that all areas of EU law are covered. This new article, which completely reshapes the landscape of data protection, takes the place of the Treaty's First Pillar Article 286 EC 37 clause on data protection. It elevates the data protection clause from "an obscure corner in the Treaty"[33] to one of its Title II Provisions with broad effect. Some significant principles are enumerated in this title, including the coherence of EU law, preventing discrimination, and public access to documents. In having general scope, it covers all processing done in the public and private sectors, including that done for police and judicial cooperation.

The treaty of Lisbon basically paved the way for the increased focus from the EU on enhancing data protection and privacy attributing at the same time new powers for Parliament, which becomes co-legislator playing a key role in the subsequent reforms. As a co-legislator and author of resolutions and own-initiative reports that sought to ensure that EU individuals would have access to a high degree of data protection, the EP was a crucial player in these reforms, and as important has been the European Court of Justice which significantly contributed to the creation of the EU data protection framework.

2.3.2. European Commission Proposals (2012)

As mentioned, even though the Data Protection Directive guaranteed effective protection of the fundamental right to data protection, the differences in the way that each Member State implemented this instrument led to significant inconsistencies, which created complexity, legal uncertainty and administrative costs. This affected the trust and confidence of individuals and the competitiveness of the EU economy[34], therefore, the European Commission decided to initiate a reform process in 2012. The new proposed Regulation aimed to strengthen individuals' control over their personal data, introduce stronger obligations for data controllers and processors, and harmonize data protection rules across the EU. Measured against the innovation cycle of the modem information society, the

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

[33] *Ibid*, at 1515.

[34] European Commission, Q&A on the Data protection Reform, Brussels, 21 December 2015

European Data Protection Directive (EDPD) began to be perceived to the most as an ancient regulatory instrument[35], which led to the Commission to issue a Communication regarding "a comprehensive approach on personal data protection in the European Union"[36] in late 2010. The modernizing themes from the Communication are continued in the 2012 draft of the Regulation ("Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data or General Data Protection Regulation), and Recital 7 properly notes that the EDPD's core goals and guiding principles are still valid despite the need for reform: providing a uniform protection of basic rights with regard to personal data processing as well as ensuring the free movement of such data between Member States.

Moreover, the proposed change to a Regulation's instrument bore both symbolic and legal significant implications[37]. In a symbolic sense, the modification reflects the Commission's view that the EDPD did not sufficiently harmonize the Union's data protection laws (Recital 7), as well as its desire for greater legal certainty and a stronger legal fusion in order to advance a single market without limiting the free flow of data (Recital 11). In terms of substantive law, the modification to a Regulation put to rest the controversy over whether the – at the time – current EDPD should be fully or minimally harmonized. Furthermore, national lawmakers would have mainly been prevented from passing particular rules to concretize generic data protection principles, especially in light of the Commission's broad authority to approve delegated acts.

2.3.3. Negotiations and Adoption of the GDPR (2016)

After years of negotiations and revisions, the General Data Protection Regulation (GDPR)[38] was officially adopted by the European Parliament and the Council of the European Union in April 2016 replacing and repealing the Data Protection Directive which no longer met the privacy requirements of the new digital landscape[39]. Many legal scholars believe that the GDPR's most significant contribution to EU personal data processing is the instrument itself because the moderation of EU data protection through a regulation, rather

[35] See Hornung Gernit, *'General Data Protection Regulation for Europe: light and shade in the commission's draft of 25 january 2012'*; Journal of Law, Technology and Society, 9(1), (2012) 64-81.
[36] European Commission, COM(2010) 609 final, 4 Nov 2010.
[37] Gerrit Hornung, *'A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January'*, SCRIPTed 64 (2012), at 65.
[38] 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).
[39] Christina Tikkinen-Piri, Anna Rohunen '*EU general data protection regulation: changes and implications for personal data collecting companies',* Computer Law & Security Review, Vol. 34, 2018, at 134.

than a Directive, represents a turning point for the EU, signaling a forced exit of this particular field of law from Member State to EU level[40].

The goal of the EU with this regulation is to give citizens more control over their personal data, strengthen their rights, reform how organizations view and control these data, and remove barriers to cross-border trades, allowing for easier business expansion across Europe and ensuring the free movement of personal data between EU Member States[41]. GDPR's ultimate goal is to create a high level of privacy protection in the European Union by ensuring a harmonized, unified, and sustainable approach to EU citizens' data protection[42]. The choice to change the legal instrument (from the Directive to the Regulation), entails that the new provisions would be binding in their entirety and thus have direct effect in all Member States when adopted pursuant to Article 288 (2) TFEU. It provided a two-year transition period for organizations to adapt their practices and ensure compliance. On May 25, 2018, the GDPR came into full effect, and organizations were required to meet its provisions regarding data protection, privacy, and individual rights. The era preceding the General Data Protection Regulation (GDPR) witnessed significant legal developments that laid the groundwork for the modern data protection landscape.

3. Leading cases pre-GDPR

In the era leading up to the GDPR, the Court of Justice of the European Union (CJEU) played a significant role in shaping the data protection landscape. The rulings from the Luxembourg Court offered vital insights, clarifying legal principles and setting important precedents. Notably, the Court addressed issues such as the definition of personal data, the

[40] Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, '*Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*', Journal of Cybersecurity, (2018), at 4. It is worth mentioning that GDPR admittedly contains many provisions that allow for national interpretations and approaches based on the culture, focus, and priorities of the supervising authorities, as recognized by the same authors.

[41] See Marija Boban, '*Protection of personal data and public and private sector provisions in the implementation of the general EU directive on personal data (GDPR*)', 27th International Scientific Conference on Economic and Social Development, (2018) and Sean Sirur, Jason RC Nurse, Helena Webb '*Are we there yet? Understanding the challenges faced in complying with the general data protection regulation (GDPR)*', 25th ACM Conference on Computer and Communication Security, (2018) 1-8.

[42] Gonçalo Almeida Teixeira, Miguel Mira da Silva, Ruben Pereira, '*The critical success factors of GDPR implementation: a systematic literature review'*, Digital Policy, Regulation and Governance Vol. 21 No.4 (2019), at 402.

roles and responsibilities of data controllers, the right to be forgotten, and the complex liabilities of online operators. This judicial contribution enhanced the understanding of privacy rights within the broader societal context, bridging legal interpretations with concerns related to freedom of information, national security, and technological evolution.

These paragraphs explore a series of leading cases that emerged prior to the implementation of the Regulation. Analyzing these landmark judgments provides valuable insights into the evolution of data protection laws and their implications for individuals, businesses, and regulatory authorities.

Furthermore, exploring the legal milestones pre-GDPR provides a valuable addendum to our historical perspective on the evolution of data protection, enabling us to appreciate the progress made in addressing emerging challenges in the digital era. These cases paved the way for fundamental concepts such as when a person could be deemed identifiable, who data controllers are not to mention the right to be forgotten and the clarifications around the liability of operators online. The analysis follows a chronological order.

3.1 Identification issues and Nowak v. Data Protection Commissioner

Nowak v Data Protection Commissioner[43] presents itself as a landmark decision which not only reshaped the legal understanding of what constitutes personal identification, but also carried profound implications for the delicate balance between privacy rights and data processing activities. By delving into the intricacies of this case, we can gain a deeper appreciation for the far-reaching consequences it had in defining the boundaries of personal identification within the realm of data protection.

The petitioner, Peter Nowak, was a trainee accountant who failed a specific open book accounting test administered by the CAI four times after completing the first and second level accountancy examinations issued by the CAI. They contested the exam results and handed down a data access request under Section 4 of the Irish Data Protection Act 1988 (referred to as "Irish law"), asking for all the personal information pertaining to them that was stored by the CAI. Despite sending Mr. Nowak a number of documents, CAI declined to submit their test script on the grounds that it did not include personal data as defined by Irish law. Mr. Nowak then disputed the justification offered for withholding their exam script

[43] *Peter Nowak v. Data Protection Commissioner*, C-434/16; ECLI:EU:C:2017:994

in a letter to the Irish Data Protection Commissioner. The Data Protection Commissioner of Ireland notified Mr. Nowak that no significant violation of Irish law had been found, and that the inquiry into the complaint would not proceed. The content over which Mr. Nowak attempted to exercise a right of rectification was not personal data covered by Irish law, according to the Data Protection Commissioner of Ireland. Before the Irish Circuit Court, Mr. Nowak filed a lawsuit challenging the Data Protection Commissioner's ruling. The Irish Court ruled that there was no decision against which legal action could be taken since the Data Protection Commissioner of Ireland had not opened an inquiry into a complaint. In addition, that Court determined that the lawsuit was unjustified since the exam script did not constitute personal information under Irish law. Before the High Court of Ireland, Mr. Nowak appealed the Circuit Court's ruling, and the court affirmed it. The Court of Appeal in turn affirmed the decision made by the High Court. The action launched by Mr. Nowak against the decision of the Data Protection Commissioner was found to be acceptable by the Supreme Court of Ireland, which authorized an appeal against the decision of the Court of Appeal. However, the Supreme Court of Ireland was uncertain whether an examination script constituted personal data, within the meaning of the Data Protection Directive, and therefore decided to stay the proceedings and to refer the case to the ECJ for a preliminary ruling.

According to the Court, Article 2(a) of the Data Protection Directive is to be interpreted as meaning that "an identifiable person" is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity. The Court reasoned that the term "any information" used in the Data Protection Directive's definition indicated that it had a broad reach and was not limited to sensitive or private information. As long as it was "related" to the data subject, it included both objective and subjective information in the form of opinion and assessments. Additionally, the exam had an impact on the candidate's rights and interests as well as their chances of getting the job they wanted. In cases where the test was open book, as in this one, the Court held that the written answers provided by a candidate during a professional examination constituted information that linked to that candidate by virtue of its substance, purpose, or impact. Additionally, the Court agreed with the Advocate General's Opinion that the goal of any examination was to ascertain and establish the unique performance of a particular person, namely the candidate, rather than, unlike, say, a representative survey, to gather data that was independent of that person. The Court determined that because the exam script included details on the candidate's intelligence and penmanship, it qualified as personal data. The

Court further determined that the evaluator's remarks also constituted personal data since they expressed the evaluator's assessment of the candidate's performance in the exam, particularly with regard to their expertise and knowledge in the relevant sector. The Court noted that the fact that such remarks also comprised information pertaining to the examiner could not be used to contest this determination. As long as such people could be recognized or located, the same information might be related to a number of people and qualify as personal data under Article 2(a) of the Data Protection Directive. The Court determined that the evaluation's comments were under the definition of personal data under Article 2(a) of the Data Protection Directive since they might have an impact on the candidate's rights and interests. In accordance with Article 6(1)(d) and (e) of the Data Protection Directive, the Court determined that written answers submitted by candidates for professional examinations, as well as any comments made by examiners regarding those answers, were therefore subject to verification of their accuracy and the necessity of their retention. According to Article 12(b) of the Data Protection Directive, they could be subject to correction or deletion. In order to do this, the Court determined that Article 12(a) of that regulation should grant a candidate the right of access to those responses and comments. As per the Court, the right to access would serve the purpose of guaranteeing the protection of that candidate's right to privacy with regard to the processing of data relating to them as held in the case of *YS and Others*[44], irrespective of whether that candidate did or did not have such a right of access under the national legislation applicable to the examination procedure.

2.1.3 Personal Data: the "Identifiability" criterion

The Nowak case bears numerous implications for the configuration of data protection, particularly regarding the definition of what constitutes personal data. Its identification becomes fundamental to exercise the right of access and, consequently, all other rights related to data protection.

When it comes to the definition of personal data, the heterogeneous nature of information susceptible to being considered personal data was already acknowledged in College Van Burgemeester en wethouders van Rotterdam v. E. Rijkeboer[45]. Along with this feature, the ECJ establishes three requirements that serve as a guideline for identifying certain data as personal data. Information is considered personal data if its "content, purpose

[44] Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*; ECLI:EU:C:2014:2081

[45] Case C-553/07, *College Van Burgemeester en wethouders van Rotterdam v M. E. Rijkeboer*, par. 59. ECLI:EU:C:2008:773

or effect is linked to a particular person"[46]. These criteria's existence offers a framework for specifying what information qualifies as personal data and marks significant progress when compared to the previous situation in which the information was linked to the data subject[47]. The use of the conjunction "or" indicates that any given piece of information can be classified as personal data if just one of these conditions is met with the presence of all three not being required. Nevertheless, it has been argued that when analyzing the nature of any particular piece of information, it does appear important to consider all of them. This caution is warranted because their combined analysis allows for a better understanding of the circumstances of the person whose personal data are being analyzed.

The decision was welcomed by scholars, mostly agreeing on the fact that the addition of the criteria to determine what personal data helps in achieving objective identification and, consequently, contributes to individuate the cases where subjects may exercise the powers that data protection grants them[48].

3.2 The impact of the Right to be Forgotten: Google-Spain

The case of Google Spain v. Agencia Española de Protección de Datos (AEPD)[49] decided by the European Court of Justice (ECJ) in 2014, marked one of the most significant developments in data protection law, specifically regarding the right to be forgotten and the responsibilities of search engine operators.

On March 5, 2010, Mr. Gonzalez filed a complaint with the AEPD against La Vanguardia's publisher as well as Google Inc. and Google Spain. The complaint claimed that when a user typed Mr. González's name into Google's search engine, the results displayed links to two La Vanguardia pages that revealed their personal information in relation to property attachment proceedings against them for recovering social security debts that had been settled years prior. First, they asked for the publisher to be compelled to delete or modify the pages so that any personal information pertaining to them was not there.

Second, they asked for Google Inc. or Google Spain to be compelled to delete or obscure the personal information pertaining to them so that it would no longer be displayed in search results or in connections to La Vanguardia. According to Mr. González, any

[46] *Nowak*, par. 35.
[47] *Ibid,* par. 40.
[48] In this sense, see Daniel Jove, '*Peter Nowak v Data Protection Commissioner: Potential Aftermaths regarding Subjective Annotations in Clinical Records'*, 2019.
[49] Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317.

mention of the attachment procedures involving him is now wholly irrelevant, having they been definitively concluded for a number of years already. The AEPD disregarded their initial complaint since the publishing was mandated by a court order while the case against Google Inc. and its subsidiary Google Spain was upheld because the search engines were in violation of the Organic Law No 15/1999 of December 13, 1999 on the protection of personal data (the "Spanish Law"). Given that the discovery and dissemination of the data could jeopardize the fundamental right to data protection and the dignity of persons in the broadest sense, including the desire of the person concerned for such data not to be known to third parties, the AEPD took the stance that it had the authority to demand the data to be removed and to prevent search engine operators from accessing certain types of data. The AEPD further noted that the duty may be owed directly by search engine operators without the need to remove the data or information from the website on which they appear, even when the continued use of the material on that site was permitted by a legal requirement. The National High Court of Spain halted the proceedings and referred a case to the ECJ after Google Inc. and Google Spain appealed the AEPD's ruling.

In issuing its decision, the ECJ's ruling rendered a both literal and teleological interpretation of the Directive. It clarified that search engine operators – such as Google – are not to be excluded from being considered data controllers, acknowledging the distinct role of search engines and website publishers. As data controllers, search engines were deemed responsible for the processing of personal data that appears in search results while also being qualified as the actors in respect to whom subjects may exercise their rights. Furthermore, the ruling acknowledged the distinct role of search engines and website publishers as it emphasized that the former could make data accessible on the basis of an individual’s name and could aggregate information into profiles in a manner that could affect the fundamental rights of individuals significantly. Most importantly, the ECJ also recognized the existence of an individual's right to request the removal or delisting of search engine links that contain personal information deemed outdated, irrelevant, or excessive. This right, commonly known as the right to be forgotten, empowers individuals to control the availability of their personal data online, subject to certain conditions and considerations.

3.2.1. Implementing Google Spain

The Google Spain ruling and the consequent affirmation of the right to be forgotten thoroughly impacted European organizations and prompted discussions all over the world[50], prompting them to reevaluate the intricate problems related to privacy and freedom of expression[51]. Nevertheless, the judgment was not unscathed by critics raising several legal questions, with the most heated debate pertaining to human rights. Two were the main lines of criticism presented: on one hand, it was argued[52] that the judgment almost entirely avoids discussing the specifics of these rights and the level of protection they provide, despite the importance the CJEU accords to them and, in particular, to Articles 7 and 8 of the EU Charter. While the Court persuasively argues that processing personal information based on a person's name through a search engine like Google is likely to have an impact on "a vast number of aspects" of a person's private life in general[53]", it remains unclear how the operation of a search engine is also likely to violate Articles 7 and 8 of the Charter as specific legal rights. On the other hand, it has been criticized the judgment's compliance with the ECHR, to which the EU seems to finally be close to accession after a 70 years long process. Admittedly, despite the emphasis on fundamental rights being used to encourage the application of laws governing the deletion of personal data, the CJEU actually used very little justification based on fundamental rights. It's been argued that the CJEU's unwillingness to cite the ECHR and the Strasbourg Court's case law is especially problematic, both in light of the – long-lasting yet seemingly – EU impending accession and, more broadly, because it runs the risk of upsetting the delicate constitutional balance reached in the European fundamental rights landscape to date, in which the European Convention has played a crucial role. What appears truly puzzling, nevertheless, is that had the CJEU actually delved into and cited Strasbourg's precedent rulings, it would have

[50] To better understand the reach of the Google-Spain case, see Brendan Van Alsenoy Marieke Koekkoek, '*Internet and Jurisdiction after Google Spain: the extra- territorial reach of the EU's "right to be forgotten'*, Working Paper No. 152, Leuven Centre for Global Governance Studies, (2015) and David Hoffman Paula Bruening Sophia Carter, 'The Right to Obscurity: How We Can Implement the Google Spain Decision', North Carolina Journal of law & technology Volume 17 | Issue 3, (2016).

[51] Phil Muncaster, '*Firms Already Swamped by Right to be Forgotten Requests'*, INFOSECURITY, (2012) available at https://www.infosecurity-magazine.com/news/firms-swamped-right-to-be/.

[52] See *inter alia,* Stefan Kulk and Frederik Zuiderveen Borgesius, '*Google Spain v. González: Did the Court Forget about Freedom of Expression?*', case notes, 2014; Eleni Frantziou, '*Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain'* and SL, '*Google Inc v Agencia Espanola de Proteccion de Datos'*, Human Rights Law Review, (2014), 761–777; Christopher Kuner, '*The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines*', LSE Legal Studies Working Paper No. 3/2015, (2015) 1 – 22-

[53] *Google-Spain*, par. 80.

avoided these incongruences without, admittedly, issuing a different ruling[54]: taking Axel Springer AG v Germany[55] and Von Hannover v. Germany[56] into consideration, these two cases alone could have provided a much-needed guidance for the better clarification of the reach of the ruling in Google Spain. In the cases of Von Hannover and Axel SpringerAG, well-known public figures fought to prevent media outlets from publishing (possibly damaging) details about their private lives.

In both cases, the ECHR outlined a thorough test to provide guidance on how to assess the conflict between the right to free expression (Article 10) and the right to privacy (Article 8). The ECHR specifically pointed out a six-point test[57] which would have required its thorough preliminary examination. Elements of the six-point test effectively express how the values underlying both Article 8 and Article 10 interact with one another, and it is safe to argue that if the CJEU had applied an as-thorough analysis of the facts as seen through the lenses of this test, the judgment might have left Google Spain's detractors feeling more satisfied with the ruling. Assuming that the Springer-Hannover test was indeed adopted by the CJEU, then this criteria would be failed by Google's handling of Mr. Casteja Gonzidez's data because it is not necessary to publish a 16-year-old's fully repaid debts from a non-public person in order to maintain free speech. Nevertheless, such analysis is worthwhile and would have offered legislators, scholars, and companies some truly helpful direction.

3.3 Controllership and Liabilities: Facebook Fanpages

In Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH[58], (known as "Facebook Fanpages") the ECJ goes as far as recognizing that the administrator of a fan page on Facebook can be considered (jointly with Facebook) responsible for the processing of data of visitors to the page. When Facebook Fanpage administrators create a Facebook Fanpage, they enter into a contract allowing Facebook to process information about visitors to their Fanpage for data

[54] For an in depth analysis look at David Hoffman, Paula Bruening & Sophia Carter, '*The Right to Obscurity: How We Can Implement the Google Spain Decision*', (2016) at 460 – 482.
[55] Axel Springer AG v. Germany, 39954/08
[56] Von Hannover v. Germany, 40660/08.
[57] *Ibid* par. 108 and *supra* Springer Ag v Germany par.89 . The test requires the ECHR to examine: (1*) contribution to a debate of general interest; (2) how well-known is the person concerned and what is the subject of the report; (3) prior conduct of the person concerned; (4) method of obtaining the information and its veracity/circumstances in which the [media] was published or acquired; (5) content, form, and consequences of the publication; and (6) the severity of the sanction imposed by the local courts.*
[58] Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388.

analytics purposes. They can influence this process by choosing which parameters/information about their visitors they would like to receive (eg. data on gender; age; education etc) while designating filters to define the categories of individuals whose personal data are to be processed and the criteria for this processing[59].

Wirtschaftsakademie Schleswig-Holstein is a business in Germany that deals with education and provides educational services, among other things, through a Facebook fan pag. In accordance with Facebook's non-negotiable T&C, administrators of fan pages, such as Wirtschaftsakademie, can access a feature called "Facebook Insights" to receive anonymous statistical data on the visits to their fan pages. The information is gathered through evidence files (also known as "cookies") that contain a unique user code and are saved on a user's computer or other device by Facebook for a period of two years. When the fan pages are opened, the user code, which may be linked with the connection information of people registered on Facebook, is gathered and processed. By order dated November 3, 2011, the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Data Protection Centre for the Land of Schleswig-Holstein, Germany), acting as the supervisory authority for the purposes of Directive 95/46 on data protection and charged with ensuring that the provisions adopted by Germany in accordance with that directive are being applied in the Land of Schleswig-Holstein, ordered the deactivation of Wirtschaftsakademie's fan page. According to the Unabhängiges Landeszentrum, neither Facebook nor Wirtschaftsakademie informed fans of the page that Facebook was collecting and processing their personal information through cookies. Wirtschaftsakademie decides to file a lawsuit against that decision with the German administrative courts, claiming that it was not responsible for Facebook's processing of its users' personal data and that it had not given Facebook permission to process any data that it had control over or the ability to affect. The Unabhängiges Landeszentrum should have taken action against Facebook directly, according to the Wirtschaftsakademie, rather than indirectly. The Court of Justice was then tasked by the Bundesverwaltungsgericht (Germany's Federal Administrative Court) to interpret Directive 95/46 on data protection.

3.3.1. Administrators of fanpages are controllers

In its decision, the Court of Justice begins by noting that it is undeniable in the current case that the American company Facebook and, for the EU, its Irish subsidiary Facebook Ireland must be regarded as "controllers" in charge of processing the personal data of

[59] *Ibid* par. 36.

Facebook users and people visiting the fan pages hosted on Facebook. The reasons behind and the methods used to process the data are essentially decided by those businesses. Most importantly, the Court determines that an administrator like Wirtschaftsakademie must be viewed as a controller jointly accountable for the processing of such data within the EU with Facebook Ireland as it actively contributes to determining the goals and means of processing the personal data of visitors to its fan page by defining the parameters (based particularly on its target audience and the goals of managing or promoting its own activities). The Court specifically points out that the administrator of the fan page can request demographic data (in anonymized form) about its target audience (including trends in terms of gender, age, connections and occupations), information on the target audience's lifestyles and areas of interest (including information on the purchases and online purchasing habits of visitors to its page, and the categories of goods), and information on the geographic location.

On the other hand, the Court ruled that Facebook cannot be exempted from its duty to protect personal data simply because a fan page administrator uses the platform it offers to take advantage of the related services. In accordance with the demands of Directive 95/46 on data protection, the Court claims that the acknowledgement of joint responsibility between the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that fan page helps to ensure a more thorough protection of those visitors' rights. Additionally, the Unabhängiges Landeszentrum is competent to exercise all of the authority granted to it by the national laws implementing Directive 95/46 with regard to both Facebook Ireland and Wirtschaftsakademie in order to ensure compliance with the rules on the protection of personal data in German territory.

The consequences of the ruling are relevant: when an undertaking established outside the EU (such as the American company Facebook) has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Directive 95/463 with respect to an establishment of that undertaking in the territory of that Member State, even if, as a result of the division of tasks within the group, first, that establishment (in the present case, Facebook Germany) is established in that Member State. The Court also states that where a Member State's supervisory authority (in this case, the Unabhängiges Landeszentrum in Germany) intends to exercise the powers of intervention provided for in Directive 95/46,4 with respect to an entity established in that Member State's territory (in this case, Wirtschaftsakademie) on the basis of infringements of the rules on the protection of personal data committed by a third

party responsible for the processing, that supervisory authority is competent to assess the lawfulness of such data processing independently of the supervisory authority of the other Member State (Ireland) and may exercise its intervention powers with respect to the entity established in its territory without first requesting intervention from the supervisory authority of the other Member State.

3.4 Further clarifications on controllers and processing in Jenovah Witnesses

In *Tietosuojavaltuutettu v Jehovan todistajat*[60] *— uskonnollinen yhdyskunta* (known as Jenovah Witnesses) the Court finds that even a religious community, such as the Jehovah's Witnesses acts as a controller for the processing of personal data done by the latter during their door-to-door preaching. This implies that the processing of personal data carried out in the context of such activity must respect the rules of EU law on the protection of personal data as well.

As widely known, during their door-to-door preaching, members of the Jehovah's Witnesses Community take notes on visits to people who are unfamiliar to them or the Community. The information gathered may include the names and addresses of those contacted, as well as information about their religious beliefs and familial circumstances. Without the knowledge or consent of the individuals affected, these data are collected as a memory help and to be retrieved for each subsequent visit. The Jehovah's Witnesses Community and its members coordinate and supervise door-to-door preaching by their members, particularly by developing maps from which regions are distributed between preachers and by keeping records regarding preachers and the amount of Community publications delivered by them. Furthermore, congregations of the Jehovah's Witnesses Community have a record of those who have asked not to be visited by preachers, and the personal information on that list is used by members of that community. The request for a preliminary ruling from the Korkein hallinto-oikeus (Finnish Supreme Administrative Court) essentially asks whether that community is required to follow the rules of EU Law on the protection of personal data because its members may take notes re-transcribing the content of their discussions and, in particular, the religious views of the people they have visited.

[60] Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat,*; ECLI:EU:C:2018:551.

3.4.1. Even religious groups can be considered controllers

First and foremost, the Court of Justice believes that door-to-door preaching by members of the Jehovah's Witnesses Community is not protected by the exceptions set out in EU Law on the protection of personal data. That action, in particular, is not a completely personal or home activity to which the law does not apply. The fact that door-to-door preaching is protected by the fundamental right to freedom of conscience and religion enshrined in Article 10(1) of the European Union's Charter of Fundamental Rights does not render that activity a solely personal or household character because it exceeds the preacher's private realm as a member of a religious community.

The main takeaway, however, arises from the Court's view for which the norms of EU Law on personal data protection apply to manual processing of personal data only where the data processed is part of a system or are designed to be a component of one.

In this scenario, because the processing of personal data is not done automatically, the question is whether the data processed are part of, or are intended to be part of, such a filing system. In this regard, the Court further clarifies that the concept of a'filing system' encompasses a set of personal data collected during door-to-door preaching, consisting of names, addresses, and other information about the people contacted, if those data are structured according to specific criteria that, in practice, allow them to be easily retrieved for subsequent use. It is not required for such a set of data to include data sheets, specialized lists, or other search tools for it to fit under that definition.

The processing of personal data in connection with door-to-door preaching must consequently respect the standards of EU data protection law.

3.5 Concluding the "controllership trinity", Fashion ID case

In ending what has been referred to as the CJEU's holy trinity[61], the last leading case for this analysis is Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV[62]. In this case, the ECJ ruled that the operator of a website that features a Facebook 'Like' button can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of the personal data of visitors to its website. Contrarily, Fashion ID and Facebook Ireland can both be considered joint controllers for the operations involving the collection

[61] Tobias Rothkegel, Laurenz Strassemeyer, '*Joint Control in European Data Protection Law – How to Make Sense of the CJEU's Holy Trinity A Case Study on the Recent CJEU Rulings (Facebook Fanpages; Jehovah's Witnesses; Fashion ID)'*, Computer Law Review International 2019/20, no. 6, at 166.
[62] Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV Judgment; ECLI:EU:C:2019:629

and disclosure of the relevant data by transmission to Facebook Ireland because it can be inferred (subject to the Oberlandesgericht Düsseldorf's investigations) that Fashion ID and Facebook Ireland jointly determine the means and purposes of those operations. The Court makes it clear that the owner of a website like Fashion ID, in its capacity as a (joint) controller with regard to certain operations involving the processing of data of website visitors such as the collection of those data and their transmission to Facebook Ireland, must disclose to those visitors certain information at the time of their collection, such as, for example, its identity and the purposes of the processing.

A German online clothes shop “Fashion ID” integrated onto its website the Facebook “Like” button. The result of integrating that button seems to be that whenever a visitor uses the Fashion ID website, Facebook Ireland receives their personal information, and this happens whether or not the visitor who clicked the "Like" button is a member of the social network Facebook. This transfer appeared to happen without the knowledge of the users and/or their consent. For these reasons German public-service organization Verbraucherzentrale NRW criticizes Fashion ID for sending personal information about website visitors to Facebook Ireland without their permission and in violation of the disclosure obligations outlined in the provisions relating to the protection of personal data. The body adhered to settle the case, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany), requests the Court of Justice to interpret several provisions of the former Data Protection Directive of 1995 which was still applicable to this case, having been replaced by the new General Data Protection Regulation of 2016 with effect decurring only from 25 May 2018.

3.5.1. Joint controllership and the step-based approach

In assessing that the Data Protection Directive does not prevent consumer protection associations from being granted the right to initiate or defend legal actions against someone who is allegedly responsible for a breach of the protection of personal data, the Court points out that this possibility is now specifically allowed for by the new General Data Protection Regulation.

Most importantly, the Court finds that it does not appear that Fashion ID can be regarded as a controller with respect to the data processing operations carried out by Facebook Ireland following the transmission of the aforementioned data to the latter. The Court elaborates the “phase-based approach”, finding that Fashion ID is a joint controller only with respect to two stages of the processing, namely the collection of personal data and disclosure by transmission of those data. This conclusion follows the opinion of Advocate

General Bobek[63], for which a natural or legal person may be a joint controller exclusively with regard to the operations for which it determines jointly the purposes and the means of the processing of personal data. Fashion-ID is then responsible for the collection and transmission of the personal data, but not for the subsequent processing that Facebook carries out[64] The Court further determines that Fashion-ID must inform the data subject and obtain their consent in response to the German court's inquiries regarding the division of duties among the joint controllers. However, the processing activities for which it is a (joint) controller are only the collection and transmission of personal data.

3.6 Conclusions from Luxembourg's decisions

The analyzed decisions from the Court of Justice of the European Union present many elements of continuity, with two main takeaways that stand out among the cases: first, that joint controllership does not always entail equal duties and liabilities for the controllers: rather, their responsibilities and liabilities should be assessed on a case-by-case analysis, and especially on the 'steps' of involvement of the respective controllers. The second takeaway that emerges is found in the broad interpretation given to (joint) controllership, which is grounded in the teleological goal of ensuring the "effective and complete protection" of data subjects, as first established in the Google Spain case[65].

Nonetheless, the legal literature has extensively discussed CJEU's case law on (joint) controllership, particularly the Facebook case and even more so the Fashion ID case. Some authors question whether the Court's favored "step(or phase)-based approach to controllership" in Fashion ID actually moves in that direction. Instead, they emphasize the danger of losing sight of the bigger picture of risks to fundamental rights[66], such as the commodification of data that will result from the subsequent trading of personal information for marketing and advertising[67].

---

[63] Opinion of Advocate General Bobek delivered on 19 December 2018(1) Case C-40/17 Fashion ID GmbH & Co. KG
[64] *Fashion ID*, para 76.
[65] See René Mahieu '*Responsibility for Data Protection in a Networked World: On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe',* Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 10, (2019) at 40.
[66] See Jure Globocnik, '*On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID'*, IIC - International Review of Intellectual Property and Competition Law 2019/50, no. 8 (2019) at 1038; M. Zalnieriute & G. Churches, '*When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllership*', The Modern Law Review (Forthcoming) (2020); Mara Paun, '*On the Way to Effective and Complete Protection: Some Remarks on Fashion ID'* , Journal of European Consumer and Market Law 2020/9, no. 1, (2020) at 35.
[67] Zalnieriute & Churches, 'When a 'Like' is not a 'Like': A New Fragmented Approach to Data Controllership' 83(4) Modern Law Review, 2020, at 861

Nevertheless, the purpose of data protection law expressly is to protect fundamental rights and the better functioning of the internal market which finds its core in the free-flow of data in the EU. What appears emerging from most of the literature is a desire for an oblivion of the latter in turn of an absolutization of the former, an anti-economic behavior which would lead to major issues that will be discussed in the next Chapter.

On this account, Luxembourg's direction appears clear and in line with its broader goal of establishing a regulatory environment that strikes a balance between individual data protection and the economic considerations of the internal market. This way of approaching the issues of the Union by balancing the interest at stake with the better functioning of the market, admittedly reflects a long-standing behavior which is rooted in the very origin of the EU as an economic, market-centered supranational organization, as we will witness in the next paragraphs.

4. Ben Farrand and the GDPR through the lenses of Ordo-Liberal Influence

The General Data Protection Regulation (GDPR), since its implementation, has been the subject of both praise and criticism. While lauded for its efforts to harmonize data protection laws across the European Union, detractors have expressed their main concerns over the regulation's perceived opaqueness and vagueness[68] among others. These critics argue that the GDPR's broad and often ambiguous provisions can lead to inconsistent interpretations, creating uncertainties for both businesses and individuals. While an in-depth analysis of the provisions at stake will be conducted only in the next Chapter which specifically tackles the Regulation, as a conclusion of this preliminary analysis of the background in which the GDPR is rooted, we argue that the GDPR's structure and content might reveal an intentional design that balances the need for a robust data protection with the desire to leave space for businesses to operate and foster in the digital market.

[68] Inter alia, see Jayashree Mohan, Melissa Wasserman and Vijay Chidambaram, '*Analyzing GDPR Compliance Through the Lens of Privacy Policy*' in: Gadepally, V., et al. Heterogeneous Data Management, Polystores, and Analytics for Healthcare', (2019) at 2; Svenkst Naringsaliv, '*What is wrong with GDPR?'*, (2019) at 5; Sandra Wachter, *'The GDPR and the Internet of Things: a three-step transparency model'*, Law, Innovation and Technology, 10:2, at 6.

Such an approach aligns with the broader economic philosophies and regulatory traditions within the EU, specifically an alleged[69] influence of Ordo-liberalism, which emphasizes market competition while recognizing the importance of state intervention in preventing market failures. Within this context, the influence of various schools of economic thought on EU law-making has been a subject of considerable scholarly interest[70] with many[71] considering that what has significantly shaped the approach of the EU to economic governance is Ordoliberalism.

Clearly, European legislation was influenced by a variety of theories and principles as well, as ordo-liberalism is neither the only philosophy that has impacted the construction of EU Institutions nor is it its exclusive intellectual foundation. Indeed, much of European integration involves confrontation, compromise, and adaptation between more 'German' ordoliberal ideas and 'French' dirigisme[72], and, particularly post-Maastricht, an increasing 'neoliberalisation' of internal market policies[73].

Some scholars divide socio-economic policies which came after 1945 into three categories[74]: socially-oriented ones, neo mercantilist ones and market-oriented ones. Unlike French dirigisme, which can be associated with both neomercantilism and socially-oriented policies[75], Ordo-Liberalism clearly fits into the 'market-oriented' category. This is why, in our current investigation of the legal and regulatory landscape that shaped the General Data Protection Regulation (GDPR), the principles of Ordo-liberalism emerge as such a

---

[69] Ben Farrand, '*The Ordoliberal Internet? Continuity and Change in the EU's approach to the Governance of Cyberspace'*, European Law Open, (2023), Cambridge University Press, Volume 2.

[70] For a deeper analysis, see Josef Hien, '*European Integration and the Reconstitution of Socio-Economic Ideologies: Protestant Ordoliberalism vs Social Catholicism*' (2020) Journal of European Public Policy 27 at 1368; Thomas Warren, '*Explaining the European Central Bank's Limited Reform Ambition: Ordoliberalism and Asymmetric Integration in the Eurozone*' Journal of European Integration 42 (20200) at 263; Brigitte Young, '*German Ordoliberalism as Agenda Setter for the Euro Crisis: Myth Trumps Reality*' Journal of Contemporary European Studies 22 at 276; Peter Nedergaard, '*The Influence of Ordoliberalism in European Integration Processes - A Framework for Ideational Influence with Competition Policy and the Economic and Monetary Policy as Examples'* (2013) 52331; Imelda Maher, '*Re-Imagining the Story of European Competition Law'* (2000) Oxford Journal of Legal Studies 20 (2000) at 155.

[71] Inter alia, Supra Ben Farrand *'The Ordo-liberal Internet? Continuity and Change in the EU's Approach to the Governance of Cyberspace'*; Dullien, S. and U. Guérot '*The long Shadow of Ordoliberalism: Germany's Approach to the Euro Crisis'*. European Council of Foreign Relations (2012); Vassilis K Fouskas, '*Placing Austerity in Context: The Greek Case Between Neo-Liberal Globalisation and an Ordoliberal EU*' in Leila Simona Talani and Roberto Roccu (eds), The Dark Side of Globalisation (2019), at 12 goes as far as saying "ordoliberalism dominated the process of European integration, dictating rules and norms across Europe in a typical imperialist fashion".

[72] For a deeper focus, Laurent Warlouzet,. '*The EEC/EU as an Evolving Compromise between French Dirigism and German Ordoliberalism'* (1957–1995), Journal of Common Market (2019), 77.

[73] For an in-depth analysis on the neo-liberalisation of the market, see Mark Thatcher, '*Supranational Neo-Liberalisation: The EU's Regulatory Model of Economic Markets'* in Vivien A Schmidt and Mark Thatcher (eds), Resilient Liberalism in Europe's Political Economy, Cambridge University Press (2013), 171 – 198.

[74] The origin of this categorization is found in Laurent Warlouzet, '*Governing Europe in a Globalizing World'*, London: Journal of Common Market Studies, Volume 57. Number 1. (2018). 77–93.

[75] *Ibid*, at 77.

compelling framework to interpret the EU policymakers' approach especially when it comes to the regulation of the Internet. By examining the GDPR from this regulatory standpoint, we can build a new comprehension of why it has taken its particular form and how it resonates with broader legal and economic traditions within the EU.

This analysis seeks to shed light on how the regulatory dynamics shaped by Ordo-liberal thought may have contributed to the formation of the GDPR. Moreover, by situating the GDPR within this context, we can appreciate its role as a paradigmatic embodiment of these principles in contemporary EU legislation.

Therefore, the aim is not to say that the EU is overtly ordoliberal, or that the entire legislative structure of the EU is the result of a coordinated effort by well-placed players to advance an ordoliberal objective. Instead, the intention is to show how ordoliberal ideas might have influenced the historical development of the policies of the EU concerning online platform governance, and how this has shaped what policy tackles have been considered appropriate in responding to new regulatory challenges in this sector.

The analysis is structured as follows: we will examine relevant EU treaties and academic literature to provide a comprehensive analysis of the impact of Ordoliberal ideas on the legal framework of the EU. Firstly, we will provide a theoretical overview of Ordo-liberalism, outlining its core principles and key thinkers. Next, we will explore the historical context in which Ordoliberal ideas gained prominence in Germany and their subsequent integration into the legal framework of the EU. Finally, we will analyze the influence of Ordo liberalism in specific areas of EU law-making, specifically in the regulation of the Internet. In fact, by examining the influence of Ordoliberal ideas in the law-making processes, this chapter allows us to analyze potential explanations for why the EU has taken the approach it has toward online platforms, as well as its choice of instruments, revealing continuity in thoughts and actions.

4.1 Ordo-liberalism in Europe: key principles and thinkers

As we mentioned previously, ordo-liberalism is a school of thinking that prioritizes economic order in the process of decision-making. In the context of the EU institutional evolution, ordo-liberalism refers to a collection of concepts about the state, the market, and their interaction that impacts the union's legislative and policy processes[76]. In the view of

[76] Ben Farrand, '*The Ordoliberal Internet? Continuity and Change in the EU's approach to the Governance of Cyberspace'*, at 14.

the theorists of the Freiburg School, the market is not a naturally occurring phenomenon, but an actively constructed order, in which law plays a central role[77]. Unlike "laissez-faire" liberals and neoliberals, the ordoliberals believe that a free economic order based on fair market competition, in being not a spontaneous phenomenon it requires, instead, the constant action of the state through the use of the law: the state must defend competition as a pillar of its economic constitution (Wirtschaftsverfassung), just as it defends the rule of law and individual rights as pillars of its legal constitution[78].

The economic constitution, according to ordoliberals, is both descriptive of a given sociological reality and normative of a desired legal system: the elevated position of law is all the more understandable given that the academic pivotal to the theory's creation was jurist Franz Böhm (also referred to as the "father of the original ordoliberal competition policy")[79], alongside economist Walter Eucken. In their view, the government should not intervene directly in market functions or influence outcomes; instead, it should establish a system of undistorted market competition protected by strong legal institutions that can break up cartels and monopolies' concentration of economic power[80]. Bohm's idea was that when it came to banning cartels, only the monopolies commission should have had the final say[81] and that interventions in general, if they occurred, should have only taken the form of legislation used to establish markets and then resolve disputes through legal procedures as a manner of 'correcting' when such markets were distorted.

These are the premises on which the ordo-liberalization of Europe thesis lays its foundations, arguing that the economic policy institutions of the European Union are based on an ordoliberal blueprint.

---

[77] See Walter Eucken, '*What Kind of Economic and Social System*?' in Alan Peacock and Hans Willgerodt (eds), '*Germany's Social Market Economy: Origins and Evolution'* (Palgrave Macmillan UK 1989) 31–32; Franz Böhm, '*Rule of Law in a Market Economy*' in Alan Peacock and Hans Willgerodt (eds), Germany's Social Market Economy: Origins and Evolution (1989).

[78] See Federico Bruno '*Ordoliberal ideas on Europe: two paradigms of European economic integration, History of European Ideas'*, History of European Ideas, Vol. 49, (2023) at 737.

[79] See Josef Hien, '*The rise and fall of ordoliberalism'*, Socio-Economic Review, (2023) at 6.

[80] See Friedrich A Lutz, '*Observations on the Problem of Monopolies*', in Alan Peacock and Hans Willgerodt (eds), Germany's Social Market Economy: Origins and Evolution (1989); Supra see Josef Hien, '*European Integration and the Reconstitution of Socio-Economic Ideologies: Protestant Ordoliberalism vs Social Catholicism*' at 1373.

[81] Anselm Küsters '*The Making and Unmaking of Ordoliberal Language. A Digital Conceptual History of European Competition Law*', Doctoral thesis, University of Frankfurt, (2023)

4.2 Ordo-liberalism and influence on the EU institutional regime

It is commonly argued[82] that this ordo-liberal understanding of the interactions between law, market and society affected the economic policy institutions of the EU. Strong competition policy, hard currency, no welfare state and a non-elected commission all seem to check Eucken's ten principles[83]. A pivotal role would have been played by Müller-Armack (referred to as "the most influential German in Bruxelles[84]") in the advancing ordo-liberal thought inside the EU integration program as he was assigned to the committee in charge of finalizing the Treaty of Rome discussions, which began in 1956 and one year later ordo-liberal concepts regarding the social market economy and competition were established in the Treaty. This has led to some strong opinion from scholars: Wolfgang Streeck contended that "European money, as conceived in the treaties, is ordoliberal and neoliberal money[85]"; Fritz Scharpf agreed on this view, stating that the European Union's 'economic constitution that places the rules governing economic relations and economic policy originated in Germany in the 1930s in the 'ordoliberal' variant of normative economic theory[86]'

As mentioned, ordo-liberalism is not the only philosophy that has influenced the development of the EU Institutions, nor is it its sole intellectual foundation. Furthermore, as a result of a greater emphasis on European integration and the global economy, ordo-liberalism as a school of thought has adapted and developed over this period. Nonetheless, the emphasis on market ordering and regulated self-regulation following best practices is what has remained constant in order to avoid market distortion, notably by the state, and this gets all the more evident when it comes to the context of Internet regulation as we will delve further into it in the next paragraphs.

---

[82] Supra Ben Farrand at 17*; inter alia*, see Vassilis K Fouskas, '*Placing Austerity in Context: The Greek Case Between Neo-Liberal Globalisation and an Ordoliberal EU*' in Leila Simona Talani and Roberto Roccu (eds), The Dark Side of Globalisation (2019) at 16; Kenneth Dyson and Kevin Featherstone, *The Road To Maastricht: Negotiating Economic and Monetary Union,* Oxford : Oxford University Press (1999) at 12.

[83] Thomas Biebricher '*Geistig-Moralische Wende. Die Erschöpfung Des Deutschen Konservatismus'* Berlin, Matthes and Seitz (2018), 200-207.

[84] Bernard H Moss, '*The European Community as Monetarist Construction: A Critique of Moravcsik'* 8 Journal of European Area Studies (2000), 247 - 258.

[85] Wolfgang Streeck '*Heller, Schmitt and the Euro'*, European Law Journal 21, (2015) at 365.

[86] Fritz W. Scharpf '*Towards a More Democratic Europe: De-Constitutionalization and Majority Rule'*, European Law Jorunal 23(5), (2017) at 316.

4.3 Influence on the Internet regulation: ordo-liberalism as the origin of the self-regulatory regime

Toward the end of the 1980s, Europe began to witness a substantial revolution in the field of telecommunications technology with the introduction of the Internet as a high-volume, largely distributed communications system. The advent of an "information society" was acknowledged as early as 1979 in a Commission Communication on the "Challenge of New Information Technologies"[87], the report makes no reference to the Internet, instead focusing on the usage of "terminals" in general.

Nonetheless, from the document emerges all the Commission's preoccupation around the economic implications of new technologies as well as the willing to exploit them within an environment of competition in order to promote European growth[88]. The following time these concerns were clearly addressed regarding the Internet (this time referred to as Information and Communications Technologies or "electronic mail") was in the 1993 Communication on Growth and Competitiveness[89]. In the document the Commission emphasizes how "the creation of a common information area will be primarily dependent on private sector investment" and that, therefore, "it becomes fundamental to create a legislative framework that encourages the growth of such investments"[90]. To achieve these economic goals, the ICT supported the opening up of telecommunications markets to competition, as well as ensuring universal service, standardization, protection of personal data and guaranteeing security for information systems[91].

If the ordoliberal philosophies stated in this paper were not evident enough, the Bangemann Report's[92] released thereafter only helps to highlight how these philosophical concepts impacted the programmatic framework of the EU for Internet regulation. This report was a study prepared by the Bangemann Group which was made up of private-sector specialists ranging from telecommunications providers to analytics firms to consumer electronics vendors focused on the economic rewards of new technologies rather than their possible security concerns. The Bangemann Report emphasized the importance of developing legal frameworks for private sector operators to capitalize on the benefits of the

[87] European Commission, 'European Society Faced with the Challenge of New Information Technologies: A Community Response' COM(79) 650.
[88] *Ibid*, 13–17.
[89] European Commission, 'Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century' COM(93) 700
[90] *Ibid* 112.
[91] *Ibid* 113.
[92] European Commission and Bangemann Group, 'Europe and the Global Information Society: Recommendations of the High-Level Group on the Information Society to the Corfu European Council' (1994) S.2/94.

information society and was adamant in stating how “the market will drive, it will decide on winners and losers [...] the prime task of government is to safeguard competitive forces”[93].

Admittedly, the Bangemann Report would have highly impacted the agenda for the Internet regulation efforts from the EU, with the Commission's Communication on an Initiative in E-Commerce[94] largely reiterating the Report in terms of identifying the problems confronting the EU in this area, as well as proposing solutions. According to the Communication, the Commission's job was to create the regulatory framework required to ensure a favourable business climate explicitly affirming that "the expansion of electronic commerce will be market-driven".[95] The E-Commerce Directive resulted as anticipated: legally based on Article 114 TFEU (at the time Article 95 EC) for the harmonization of the internal market pursuing principles aimed at market facilitation, Articles 12-15 of the Directive set up the framework for intermediary liability which grants a general immunity insofar as these private sector individuals acted expeditiously to remove illegal or right infringing content which took place on their services and that was brought to their attention.

4.4 Scarlet v. Netlog and Netlog v. SABAM. A matter of privacy or more of a market concern?

The interpretation of the requirements under this regulated self-regulatory framework for online intermediaries was reviewed by the Court of Justice in cases involving copyright infringements online, which were the primary focus of E-Commerce Directive litigation in the late 2000s.

Briefly recalling the cases, the matter at issue in SABAM v. Netlog was whether a Belgian court could order Netlog to stop making works from SABAM's repertoire available immediately. The Court determined that the injunction requiring Netlog to install a filtering system, which would compel Netlog to actively monitor all of its users' data and stop future IPR violations, was in violation of both the Charter of Fundamental Rights and article 15 of Directive 2000/31. Furthermore, the protection of fundamental rights of people who are impacted by such measures must be balanced fairly with copyright protection, according to national authorities (para. 43). If the injunction were to be used in this situation, it would seriously impair the hosting service provider's freedom to operate its business because it would force it to install an intricate, expensive, permanent computer system at its own

[93] *Ibid* 13
[94] European Commission, ‘A European Initiative in Electronic Commerce’ COM(97) 157.
[95] *Ibid* 1

expense, which would also be against the terms outlined in Article 3(1) of Directive 2004/48, which states that measures to ensure the respect of intellectual property rights should not be unnecessary.

Both Scarlet v SABAM[96] and SABAM v Netlog[97] were seemingly concerned with the balancing of protection of intellectual property rights with privacy rights (which has been a prominent focus of much of the literature on copyright infringement online)[98]. The two cases are mostly perceived as the first big steps of the Court towards the defense of fundamental rights and rights of internet users[99] in general, and quite rightfully so: the Court clarified how the injunction would have violated Netlog users' fundamental right to data protection while also undermining freedom of information because the system might not distinguish adequately between unlawful and lawful content, potentially resulting in the blocking of lawful communications.

However, an intriguing aspect of these judgments that has garnered less attention is the Court's contention that the responsibility to safeguard copyright must be weighed with a company's rights to conduct business. Although discussed as an obligation arising from Article 16 of the European Charter of Fundamental Rights, as O'Sullvian[100] points out, this right in its entirety is the freedom to conduct business in accordance with Community and national laws, and thus qualified rather than absolute, as the Court does not emphasize. The reference is more relevant in the context of this analsys as a reflection of ordoliberal philosophy that interference in market activity should be limited, deferring to the Internet intermediary self-regulatory regime, as highlighted in the UPC Telekabel[101] case, where the Court inferred that any obligations to implement measures such as website blocking granted under an injunction should leave the addressee free to establish the particular steps to be followed in order to accomplish the desired objective, with the result that he can choose to put in place measures that are most suited to the resources and abilities at his disposal[102].

---

[96] Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) EU:C:2011:771

[97] Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV EU:C:2012:85

[98] See for example Paddy Gardiner and Gillie Abbotts, '*Scarlet Extended Reprieve from Content Filtering'* ,Entertainment Law Review, (2012) at 75; Evangelia Psychogiopoulou, *'Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers after Scarlet'* European Intellectual Property Review 34 (2012), at 552; Kevin P O'Sullivan, '*Enforcing Copyright Online: Internet Service Provider Obligations and the European Charter of Human Rights'* European Intellectual Property Review 36 (2014), at 577.

[99] *Inter alia,* see Laurens Ankersmit, *'Case C-360/10 SABAM v. Netlog'*, European Law Blog, (2012)

[100] Supra Kevin P O'Sullivan, *'Enforcing Copyright Online: Internet Service Provider Obligations and the European Charter of Human Rights'*.

[101] Case C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, ECLI:EU:C:2014:192.

[102] *Ibid*, para.52

4.5 The Ordoliberal internet: Influence on GDPR

Drawing from an ordoliberal philosophical starting point regarding market structuring, resulting in a programme of private sector expertise and non-interventionist approaches to market order, regulation of the Internet has been typified by forms of regulated self-regulation, in which the market operators are seen as both expert and best placed to regulate their own activities on the Internet. Building upon this premises, the General Data Protection Regulation (GDPR) represents the result of a progressive evolution of ordoliberal ideas in the context of data protection and privacy regulation.

While the GDPR focuses specifically on the protection of personal data, it aligns with several prerogatives of ordoliberalism, such as establishing and maintaining a competitive market economy that safeguards individual freedoms and social welfare. One key aspect where this phenomenon emerges the most is the focus on empowering individuals and enhancing their control over their personal data, which is at the very basis of the Regulation.

In the analysis made in this Chapter of the regulations adopted and the case law in both Luxembourg and Strasbourg, we have witnessed how the different European institutions and organisms all have seemingly tended toward a common direction, this being the control of users over their data. The regulation provides a comprehensive framework in this sense, providing individuals with rights such as the right to be informed, the right of access, the right to rectification, the right to erasure, and the right to data portability. All of these rights empower individuals to exercise control over their personal data, ensuring transparency, and granting (at least in principle) them the ability to make informed choices regarding the use and processing of their information. This also resonates with ordoliberal principles that prioritize individual freedom and autonomy within the framework of a competitive market economy.

Moreover, the GDPR's emphasis on accountability and transparency appears to align with ordoliberal concerns for ensuring fair competition and preventing market distortions. The regulation places obligations on organizations to implement privacy-by-design principles, conduct data protection impact assessments, and maintain records of data processing activities. These requirements promote responsible data practices, preventing the concentration of market power in the hands of a few dominant players and ensuring that businesses operate in a transparent and accountable manner. By doing so, the GDPR strives to foster fair competition and protect individuals from potential harms resulting from unchecked data practices, in line with Ordoliberal principles.

5. Concluding remarks

In this chapter, we have explored the legislative path leading to the General Data Protection Regulation (GDPR). Our analysis began by examining the initial steps taken in the development of data protection laws, notably with the precursor to the GDPR, Convention 108, and the EU Data Protection Directive. These early legislative milestones laid the foundation for the extensive framework that would later become the GDPR.

Furthermore, we delved into significant legal cases that emerged prior to the GDPR, illustrating the evolving landscape of data protection in the European Union through the decision of Luxembourg. The landmark "Google Spain" case, along with other notable cases such as Nowak v. Data Protection Commissioner, Facebook Fan Pages, Jenovah Witnesses, and Fashion ID, showcased the complex legal issues surrounding data privacy and their impact on individuals and organizations, and most of all, the direction that the Court has intended to take.

Finally, we explored the influence of ordoliberal ideas in the EU law-making processes. Ordo-liberalism, a significant economic and political philosophy in Europe, has played a noteworthy role in shaping regulations and policies, including those related to internet regulation and data protection.

Our analysis leads us to consider the GDPR as a regulatory instrument that has been shaped by various factors. Among these, historical legal developments, significant judicial decisions, and an awareness of ordoliberal principles stand out. Simultaneously, the consideration of ordoliberal principles in the approach of the EU to regulation may be seen as a lens through which the GDPR was fashioned. This nuanced interplay reflects an understanding by the European legal and regulatory authorities of the need to balance personal data protection with the functionality of the internal market. This perspective forms the basis for our further exploration of specific provisions and implications of the GDPR and explore its impact on various stakeholders, including individuals, businesses, and regulatory authorities.

CHAPTER II - STRIKING THE BALANCE BETWEEN THE BETTER FUNCTIONING OF THE INTERNAL MARKET AND PRIVACY ISSUES

1. GDPR: between Data Protection and Free Movement of data

Article 1 opens the Regulation stating that it "*lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*[103]. Building upon our previous exploration of the legislative path towards the General Data Protection Regulation, this chapter aims to delve into the intricate balance that the GDPR strikes between protecting personal data and facilitating the free movement of such data within the European Union (EU).

At five years from its entry into effect, we will tackle the objects of the main critics moved towards the Regulation revolving around the vagueness of its provisions, the insufficient protection for privacy rights in the EU and in transfers abroad and the difficulties in enforcement[104]. The aim is demonstrating the importance of considering the regulation's dual objectives., despite the inherent challenges presented by the contrasting interests of data protection and the best interests of the internal market.

In the upcoming paragraphs, we will begin our analysis by briefly taking into account the main principles and aims of the GDPR. Afterwards, we will explore the notion of the free movement of data as a – much needed – "fifth freedom", which goes to complete and prove itself as a valuable addition to the traditional freedoms of movement within the EU with a parenthesis on the concept of data as a monetary value, recognizing its economic significance and the implications for the data protection landscape. All in all, we will emphasize the fundamental importance of freedom of data movement in our data-driven economy, elucidating how it underpins innovation, economic growth, and the development of digital services. The analysis will than proceed tackling the privacy framework and how

[103] Art. 1 GDPR.
[104] See Giulia Gentile and Orla Lynskey, '*Deficient by design? The transnational enforcement of the GDPR. International and Comparative Law Quarterly'*, Vol. 71 No.4, (2022), at 800.

the two interests are being dealt with in practice by the Court of Justice. The aim is to prove whether the provisions laid down by the GDPR are capable of striking a good balance between these two seemingly opposite interests[105] providing a comprehensive understanding of the Regulation's efficacy and its impact on both the business landscape and individual privacy from which conclusions will be drawn.

1.1 Premises: Regulation's structure and data processing activities

The General Data Protection Regulation is structured into 11 Chapters and 99 Articles that are are complemented by the 173 Recitals which provide clarifications, context, and explanations to aid in the interpretation of the legislation. Personal data and information activities considered 'processing' are two threshold definitions. GDPR defines personal data as "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 of an identifier (…)"[106]. As a result, the GDPR's definition of personal data extends far beyond personally identifiable information such as names and addresses. In a nutshell, personal data is any datum that identifies or could identify a person in the future. Public and non-sensitive information can also be considered 'personal data,' as can pseudonymous identifiers[107], IP addresses, tracking cookies, and other similar information. The GDPR also added 'location data' and 'online identifiers' to the GDPR's personal data definition as examples of identifiers.

The Regulation applies when such personal data is processed, activity described as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (...)"[108]. This involves operations like collecting, storing, disclosing, and erasing data and it is not uncommon the idea for which practically everything that can be done with personal data can be considered "processing"[109].

[105] For an in-depth analysis of the challenges that such a balancing may pose, see Bart Custersa,, Gianclaudio Malgieri, '*Priceless data:why the EU fundamental right to data protection is at odds with trade in personal data',* Computer Law & Security Review, Volume 45, (2022) 1-11.
[106] GDPR art 4(1).
[107] GDPR rec 26.
[108] GDPR art 4(2).
[109] Chris Jay Hoofnagle, Bart van der Sloot, Frederik Zuiderveen Borgesius, '*The European Union General Data Protection Regulation: what it is and what it means'*, Information & Communications Technology Law, (2019), at 72.

The most important actors figuring in the GDPR are four, namely the data subjects (the natural persons whose personal data are processed[110]), controllers (those who determine the purposes and methods of processing[111]), processors (entities operating with personal data on behalf of the controllers[112]) and the Data Protection Authorities.

These are independent authorities set up to monitor the consistency of its application "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[113]". DPAs serve as the enforcement arm of the GDPR, ensuring that both companies and individuals are adhering to the laws and regulations that have been set forth to protect personal data. The delicacy of their task can be better understood by recognizing the dimensions of fines under GDPR can achieve.

There is a broad consensus among scholars[114] that enforcement can be deterrence or compliance-driven, with the latter requiring those regulated to be aware of the possibility of enforcement and it entails issuing fines and sanctions for not complying with the regulations[115]. In crafting the GDPR, policymakers definitely adopted a deterrence-driven strategy, being the Regulation designed to be the toughest privacy law in the world[116]. GDPR fines are declined into two categories both enshrined into Article 83. Paragraph 4 of the article refers to the infringements[117] which are subject to administrative fines of up to EUR 10,000,000.00 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Paragraph 5, instead, sets out the infringements for which are levied administrative fines of up to EUR 20,000,000.00 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Moreover, even though the Regulation was drafted and passed by the EU, it imposes obligations onto organizations anywhere, so long as they target or collect data related to

---

[110] GDPR Art 4(1).
[111] GDPR Art 4(7)
[112] GDPR Art 4(8).
[113] GDPR Art 51.
[114] Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills, '*Data Protection Authorities and Their Awareness-Raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-Size Enterprises*' European Data Protection Law Review (EDPL) (2020) at 352
[115] For more on enforcement strategies see: Robert Baldwin and Martin Cave, '*Understanding Regulation: Theory, Strategy, and Practice'* Oxford University Press, (1999) and Neil Gunningham, *'Enforcement and Compliance Strategies',* in The Oxford Handbook of Regulation, (2010).
[116] Inter alia, Karen Painter Randall, '*GDPR makes the EU the toughest on data privacy'*, TELFA (2018) and Adam Satariano, '*G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog'*, The New York Times, (2018).
[117] GDPR Art 83(4), these infringements are: the obligations of controller and processor in connection with the conditions for a child's consent under Art. 8 GDPR – Art. 11 GDPR; the organizational requirements for processing under Arts. 25 to 39 GDPR; data protection Certifications under Arts. 42, 43 GDPR; the obligations of the certification body pursuant to Arts. 42, 43 GDPR; the obligations of the monitoring body for Codes of Conduct pursuant to Art.41 Sec. 4 GDPR

people in the EU. In giving away the Regulation's extensive territorial scope, Article 3 establishes that the rules apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This means that the GDPR's reach is not confined to the geographical boundaries of the EU, rather, it extends to any organization worldwide that processes the personal data of individuals residing in the EU. Whether a business is based in North America, Asia, or any other region, if it collects or processes data related to EU citizens, it is obligated to comply with the GDPR.

Stemming from these surface-level considerations on the structure of the Regulation, we will now delve into the main principles that guide the data protection landscape.

1.2 Premises: main principles and aims of the Regulation

To safeguard data protection, the GDPR establishes a robust set of principles enshrined in Article 5. The principles of lawfulness, fairness, and transparency shape the very core of the discipline, being all inherently linked with each other[118]. Fairness and lawfulness principles go hand in hand, with the latter imposing on organizations not to withhold information about what data they are collecting and provide the reasons why while the former ensures that such data is not misused or poorly handled. Article 6 further develops the principle of lawfulness by providing six grounds on which any processing activity must be based in order to be considered lawful, namely: the (data) subject's consent (1)(a)), the necessity of contract performance (1)(b)), the necessity to comply with a legal obligation on the controller (1)(c)), the necessity to protect the data subject's vital interests (1)(d)), the necessity to perform a task carried out in the public interest or the exercise of official authority (1)(e)). While it appeared to the most that the Article goes only to replicate what already provided in the Data Protection Directive, it should be highlighted how it goes much beyond [119], providing a much more comprehensive framework in regard to consent. In fact, notwithstanding the five "necessities", the true cornerstone of data protection discipline in Europe is indeed consent, which needs to be both freely given and informed as enshrined in

[118] GDPR, Art 5.
[119] See Elena Gil González, Paul de Hert, '*Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles'*. ERA Forum 19, at 601 (2019).

Article 4 while also "unambiguous" as well. Giving consumers true choice over how their data is used is what the requirement for free consent entails. As a result, the controller must allow for distinct consents for different processing operations[120], and consenting to provide more data than necessary cannot be a condition of contract provision[121].Informed consent is also linked to the principles of fairness as well as to the information requirements outlined in Articles 13 and 14 GDPR (which require the controller to inform about, among other things, the purpose of processing and the lawful basis or existence of automated decision-making). In online environments, this is typically accomplished through privacy banners, which have long been criticized – and rightfully so – of being overly too complex or even incomprehensible to the average user[122], to the point that many argued that they account for an "un-informed consent" at best[123]. Nevertheless, it is undeniable that in some way, this approach served its purpose, this being making the public aware of the risks behind the processing: as someone noted[124], while notices are poor at informing people, they can be excellent at raising the necessary skepticism to prevent misplaced trust. Secret or cloaked-in-secrecy information practices are inherently unreliable. Even if they aren't entirely certain of what they are avoiding or how likely an unwanted action or effect is, skeptics act more cautiously or completely refrain from accepting risk when faced with such practices.

Letter b of Article 5 follows by introducing the principle of purpose limitation. Just like consent, purpose comes with its mandatory requirements: it must be specified, explicit and legitimate. The initial aspect of the purpose limitation rule is the obligation that the controller must specify the purpose or purposes that are intended to be served with the obtained data while collecting the data[125]. Article 29 Working Party also clarify that granting a sufficient degree of specification depends on the environment in which the data is obtained and must be decided for each specific case. In some cases, simple statements of the aim are sufficient, whilst others necessitate a more extensive specification[126]. By explicit, on the other hand, the provision entails that the purpose specification must be properly revealed and described or articulated in an understandable manner no later than the time the personal

[120] Recital 43 GDPR and Art. 29 Working Party
[121] Art. 7(4) GDPR and Art. 29 Working Party
[122] *Inter alia*, see Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub and Thorsten Holz. *'(Un)informed Consent: Studying GDPR Consent Notices in the Field*', Conference on Computer and Communications Security (2019) see also Martin Kirsten, '*Privacy notices as tabula rasa: an empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online'* J. Public Policy Mark. 34(2), at 210 (2015)
[123] *Ibid*.
[124] Neil Richards & Woodrow Hartzog, '*Taking Trust Seriously in Privacy Law'*, 19 Stanford Technology Law Review 431 (2016), at 463.
[125] Art. 29 WP, p. 15.
[126] *Ibid*. p16.

data is collected. This requirement is all the more fundamental as it contributes to both transparency and predictability by allowing third parties to understand how personal data can be used and indicate the boundaries of personal data processing[127]. Finally, the purpose for which the data has been obtained must be legitimate. Once again this partially pertains the general norms drawn from Articles 7 and 8 DPD, namely that the processing of personal data is banned unless there is a legal reason, such as the data subject's agreement. Furthermore, the provision mandates that all applicable laws, customs, standards of conduct, codes of ethics, and contractual arrangements must be followed.

Data minimization principle (1)(c) requires the processing of only personal data to be adequate, relevant, and not excessive in connection to the purposes for which the data is acquired and/or further processed. As a result, after identifying the objective, the data controller must carefully examine whether the collection and/or processing of personal data is required for the aim. Adequacy is arguably the most intriguing of the three criteria because it may actually (and as it has been noted rather counterintuitively[128]) necessitate greater data processing.

Letter d of the Article calls for the accuracy of the data and where necessary, kept up to date, while letter f for the integrity and confidentiality of the processing. Letter e is the only segment of the provision where the processing activity is not addressed directly as it refers to the period of storage of the data which must be no longer than necessary with this having as a parameter once again the purposes of the controller.

The second and last paragraph of Article 5 establishes the principle of accountability, deeming the controller responsible of ensuring compliance with all of the above. This inextricable link to all six other principles has made scholars believe that accountability is the real core of the Regulation[129] as the imposition of sanctions works best when the process of accountability (and the relationship agent-principal) is clearly established rendering the evaluation easier[130]. Moreover, the accountability principle underpins the GDPR's hybrid

[127] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, '*The Principle of Purpose Limitation and Big Data*', Chapter in 'New Technology, Big Data and the Law', Kyushu University (2017), at 27.
[128] See Asia J. Biega, Peter Potash, Hal Daumé, Fernando Diaz and Michèle Finck, '*Operationalizing the Legal Principle of Data Minimization for Personalization*' in Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (2020), at 400.
[129] See Paul de Hert and Guillermo Lazcoz, '*When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance*', European Data Protection Law Review 8(1) (2022) at 32.
[130] On the discussion on whether the possibility of sanctions is a constitutive element of accountability, see Mark Bovens, '*Analysing and Assessing Accountability: A Conceptual Framework',* 13 European Law Journal 4, (2007) at 447-468.

approach to data protection governance[131]: the Regulation defines the principles that data controllers must follow, although it is mostly up to them how they achieve such outcomes, under the supervision of public guardians[132]. In this context, Article 24 GDPR requires the controller to be accountable for *the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, and to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the data processing is performed in accordance with this Regulation.* Because of the risk created by the processing, the GDPR imposes both specific mandatory technological or organizational precautions in particular situations (for example, when processors use automated decision making, which is in principle forbidden by Article 22(1) GDPR) as well as discretionary measures that may be adopted when the controller considers them necessary for the reasons listed in Article 24(1).

In conclusion, the principles enshrined in Article 5 of the GDPR aim to form a comprehensive and balanced framework that guides data controllers in their responsible handling of personal data. This framework provides instructions and standards to ensure the lawful, fair, and transparent processing of data, with a strong emphasis on safeguarding individuals' privacy rights. By granting data subjects the autonomy to provide or withdraw their consent, the GDPR recognizes and respects their right to control the use of their personal data. This consent-based approach fosters trust and confidence in data processing practices, promoting a secure and privacy-conscious digital ecosystem.

Moreover, the GDPR's flexible yet accountable framework grants leeway to data controllers, acknowledging the diverse nature of data processing scenarios. This flexibility encourages innovation, economic growth, and cross-border business activities within the EU. The regulation's ability to harmonize the interests of data subjects and data controllers is a proactive effort to create a thriving data-driven economy.

Looking ahead, the delicate balance achieved by the GDPR in protecting personal data while fostering the free movement of such data is paramount to what we argue to be Regulation's overall success. In today's society, the seamless and free movement of data is a fundamental aspect that drives innovation, competition, and economic prosperity. As such, the next paragraph will delve into why the free movement of data is crucial in our data-

[131] Karen Yeung and Lee Bygrave, *'Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship',* Regulation and Governance 19, (2022) at 1.
[132] Ugo Pagallo and others, *'On Good Al Governance: 14 Priority Actions, a S.M.A.R.T. Model of Governance, and a Regulatory Toolbox*', Working Paper, (2019) at 24.

driven economy and explore the benefits it brings to businesses, consumers, and the internal market as a whole.

1.3 Freedom of movement of data: the "fifth freedom" and why it is necessary

Article 1 of the GDPR opens by giving away the double scope of the Regulation, this being laying down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. While most of the scholars' attention has been given to the former scope, we argue that the discipline laid down to ensure the free movement of personal data within the EU bears no less importance. Stemming from the freedoms already in place in the Treaty on the Functioning of the European Union (TFEU), namely the free movement of goods, capital, services, and workers, the provision establishes what has been referred to as a fundamental "fifth freedom[133]", consolidating the idea for which data already counts as one of the principal factors of production[134] .The same Article 1(3) of the Regulation doubles down on the relevance of the topic, establishing how "*the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*". This provision appears to signify that while the GDPR imposes strict rules and obligations on the processing of personal data to protect individual privacy, these rules should not serve as a pretext to restrict or prohibit the free flow of data within the EU.

In laying down one of the Union's objectives, Art. 179 TFEU[135] expressly mentions the strengthening of its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely. The establishment of this "fifth freedom" appears to drive specifically in this direction, as achieving these ambitious goals profoundly necessitates free movement of personal data

[133] See Kaspar Kala, '*Free movement of data as the 5th fundamental freedom of the European Union'*, published on e-Estonia, (2017).
[134] The idea is more fully developed in Paul Hofheinz and Michael Mandel, '*Uncovering the Hidden Value of Digital Trade: Towards a 21st Century Agenda of Transatlantic Prosperity',* Interactive Policy Brief 19/2015, (2015).
[135] Consolidated versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, C326, art. 179, (2012).

relating to patients and research participants[136] among others. Data sharing across borders is, in fact, frequently essential as building a large enough cohort to achieve meaningful clinical results and statistical significance may be required for research. Also, obtaining an expert opinion from outside the country may be critical in the case of health care. This is also why GDPR aims to eliminate any concerns about processing personal data across EU borders.

In a real case-scenario, a university hospital in Germany that shares health data about research participants with a collaborating pharmaceutical company in Greece can be confident that the data will be processed in Greece under the same legal regime as in Germany, in both the private and public sectors. Additional rules may be imposed by member countries, but none may impede free data flow.

It is also worth emphasizing how, building up from the freedom connected to the movement of personal data, the EU decided to broaden it to non-personal data as well. Non-personal data, in fact, can still be processed to influence individuals' behaviour, in which case, given the purpose for which it is used, certain DPAs may consider the data to be personal data under the current status quo[137]. This addendum brings with it useful guidance as well as the completion of the EU strategy to make data (be it personal, anonymous, pseudo-anonymized or non-personal) freely moving and uniformly processed in the EU.

1.3.1. Free Flow Regulation to ensure freedom of movement of all data

In recognition of the possibility that obstacles to the free cross-border movement of data within the EU could slow or impede the growth and innovation arising from the European data economy, a proposal for a Regulation on the free flow of non-personal data in the EU[138] (also known as NPDR or Free Flow Regulation) was presented by the European Commission in 2016 and then adopted on November 14, 2018. Its rationale is basically to complete and complement the GDPR by taking into account all the data that is not already covered by the Regulation, this being the non-personal data. At first, the NPDR's utility was

[136] See Heidi Beate Bentzen and Njål Høstmælingen, '*Balancing Protection and Free Movement of Personal Data: The New European Union General Data Protection Regulation'*, Annals of Internal Medicine, (2019) at 335 (emphasis added).
[137] For an in-depth focus on the relevance of non personal data and its relationship with the discipline laid down in GDPR, see Nicoleta Cherchiu, Teodor Chirvase, '*Non-personal data processing – why should we take it personally?*', European journal of Privacy Law & Technologies, (2020), 183 – 192.
[138] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, ELI: http://data.europa.eu/eli/reg/2018/1807/oj

questioned from scholars as the notion of personal data is admittedly far-reaching[139]. Its extent was clarified to a certain degree in the case *Breyer*[140] where the European Court of Justice ruled that personal data under Article 2(1)(a) Directive 96/45 is defined as information relating to an identified or an identifiable natural person. Also, an identifiable person is one who can be identified directly or indirectly by reference to an identification number or to one or more factors that are specific to the person's physical, physiological, mental, economic, cultural or social identity. The Court basically made it clear that information can be considered personal data whenever additional information about a data subject can be obtained from third parties.

Nonetheless, the Free Flow Regulation introduces some key provisions, such as the general ban in EU for data localization requirements enshrined in Article 4[141]. These are described as any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law.

1.3.2. Data Localization requirements removal and benefits

Historically, the existence of so-called "data localization requirements" has hampered the free flow of data and can take several different forms as they may be applied to personal or non-personal data, but they may also be applied uniformly to all data types regardless of their classification. A requirement for data localization, however, essentially restricts the transfer of data from one nation to another, therefore they all share one thing in common: they increase the price of international business[142]. In the EU, over 60 of these restrictions were found in 25 different countries[143]. For example, data localization requirements have a particular impact on cloud service providers. They contend that these limitations undermine the cloud business model by preventing users from using cloud services offered by another

[139] See Bird&Bird Insights, '*Big Data issues & Opportunities, Free flow of Data'*, (2019).
[140] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
[141] Free Flow Regulation, Art. 3.
[142] Martina F. Ferracane, *'Restrictions on Cross-Border Data Flows: A Taxonomy*', ECIPE Working Paper, No. 1/2017 14 (2017) at 23.
[143] S*e*e p.37 of Annex 5 to the Commission staff working document impact assessment, citing: LE Europe study (SMART 2015/0016) and TimeLex study (SMART 0054/2016) (Commission, 'Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' (Staff Working Document) SWD (2017) 304 final.

EU Member State or by preventing providers from entering markets where they do not have a data center[144]. Nevertheless, legislators or policymakers frequently impose these restrictions because they believe that data is safer stored within a nation's borders. A misconception, as data security is dependent more on the specific security measures used to store the data than it is on the physical location where the data is stored[145]. Security measures are equally effective or ineffective abroad as they are at home, or put another way, a secure server in Poland shouldn't be distinct from a secure server in Belgium.

Thus, the need for data localization limits the availability of less expensive and more innovative services for businesses and government agencies or forces multinational corporations to outsource excess data processing and storage capacity. This poses a significant barrier to growth, market entry, and the creation of new goods and services for start-ups and SMEs (including those in the transportation industry)[146].

Furthermore, the NPDR provides that EU Member States won't be able to limit the location of data processing activities to a specific Member State's territory or achieve the same result by imposing limitations on the processing of data in other Member States. Data localization requirements could only be accepted in exceptional cases, when justified on the basis of public security and taking the proportionality principle into consideration and finally that Member States shall make the details of any data localisation requirements laid down in a law, regulation or administrative provision of a general nature and applicable in their territory publicly available via a national online single information point which they shall keep up-to-date, or provide up-to-date details of any such localisation requirements to a central information point established under another Union act.

[144] European Commission, *'Annex to the Synopsis Report. Detailed Analysis of the Public Online Consultation Results on 'Building a European Data Economy*' (European Commission 2017) at 3-4.
[145] Daniel Castro, *'The False Promise of Data Nationalism'*, The Information Technology & Innovation Foundation (2013), at 1.
[146] Commission, *'Building a European Data Economy'* (Communication) COM (2017) 9 final, 6-7.

1.4 Benefits stemming from the free movement of data

GDPR's framework completed by the provision of NPDR, combined with other important instruments such as the NIS Directive in the field of Cybersecurity[147] (now NIS 2[148]) create a rather fertile ground for the better functioning of the EU internal (and, more specifically, digital single) market. Over time, in fact, personal data have risen in value in comparison to goods and services, if not even exceeding them[149], making it just as necessary for the sake of the internal market and EU businesses to make their transfer expeditious and free. Together, these regulations create a dynamic data-driven ecosystem that empowers businesses, benefits consumers, and fosters a thriving digital economy. The aim of this thesis is also to delve into the reasons behind the fundamental importance for Europe in maintaining and further fostering such an environment in nowadays' landscape. The seamless cross-border data transfers benefit the market in numerous ways, allowing companies to access diverse datasets, fueling advancements in technologies like AI and machine learning, while also promoting digital transformation. Not less importantly, the free flow of data encourages cross-sectoral collaboration, allowing industries such as healthcare and energy[150] to leverage shared data for groundbreaking discoveries and resource optimization. These are only some of the many reasons why "free movement of data" has become so important[151] - European citizens, businesses, and even countries cannot thrive in this environment on their own[152] They must collaborate to gain access to large data sets that will enable analytics to propel and keep Europe at the forefront of the data-driven economy.

The Regulation, by enabling businesses to operate across EU member states with some degree of ease, goes to enhance market integration and contribute to the development of a harmonized EU digital single market. The availability of vast datasets not only enables

[147] For insights on the interplay between NIS Directive and GDPR, see Dimitra Markopouloua, Vagelis Papakonstantinoua, Paul de Hert, '*The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation', C*omputer law & security review 35, (2019).

[148] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); ELI: http://data.europa.eu/eli/dir/2022/2555/oj

[149] Costa-Cabral Francisco and Lynskey Orla '*Family ties: the intersection between data protection and competition in EU Law*' Common Market Law Review, 54 (1), 2017, at 11.

[150] See Opendei Energy Domain Study, '*Data Spaces for Energy, Home and Mobility'.* In Abstract, referring to the Digitalisation of Energy Action Plan (DoEAP) (at 1): "*Data exchange is crucial for emerging energy data services in the digital energy market and will help suppliers and energy service providers to innovate and cope with an increasing share of renewables in a more decentralised energy system".* As to healthcare, In order to unleash the full potential of health data, the European Commission is presenting a regulation to set up the European Health Data Space https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197

[151] See Paul Hofheinz and David Osimo, *'Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age'*, The Lisbon council, Policy Brief at 5.

[152] European Commission, *Building a European Data Economy*, Brussels: European Commission, 2017.

personalized consumer experiences but also improves various aspects of daily life through data-driven services.

Even what was initially addressed as a possible threat, like consent requirements, actually bears opportunities. Under GDPR, as we have seen, organizations need explicit consent to store and process personal data. Due to the smaller addressable audience, this may initially appear to be a threat to the marketing and sales pipeline, but there is a benefit. The value of each individual contact will significantly increase if the company has a smaller list of contacts who have all expressed a desire to hear from it[153]. This benefits both businesses and customers. Customers will receive less spam and "grey mail," and businesses will spend less time and money on contacts who are not genuinely interested in their goods and services. As a result, they can concentrate on those who have shown a genuine interest. Marketers will notice a rise in the rate of engagement with their messaging as a result. It is more valuable to send a marketing email to 100 recipients and get half of them to interact with it than to send it to 200 recipients and get no interactions at all. Lead management will become more effective as marketing shifts its emphasis from producing the most leads possible to producing higher quality leads. Sales teams will receive higher quality leads that have a greater chance of closing than in the past. That said, the benefits stemming from the framework provided by the GDPR is not only business-oriented but take into consideration many other dimensions as we will see in the next paragraphs.

1.4.1. Benefits for research

As mentioned, the Regulation contributes to the fulfilment of the objectives enshrined in Article 179 of TFEU, promoting a trustworthy and fair framework for data sharing and related research goals as well, even though the majority of scholars split between those who see the GDPR as a direct hindrance to research[154] to those who see the absence of clear interpretive guidelines for research as the real hindrance to scientific progress[155].

[153] See '*Three Key Risks and Opportunities of GDPR'*, Comforte AG, (2018), at 6.
[154] See David Peloquin, Michael Di Maio, Barbara Bierer, Mark Barnes, '*Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data',* European Journal of Human Genetics, (2020) at 1; Tania Rabesandratana, *'European Data Law is Impeding Studies on Diabetes and Alzheimer's*, Researchers Warn' Science (2019); Birgit A. Simell et al., '*Transnational Access to Large Prospective Cohorts in Europe*: *Current Trends and Unmet Needs*' , 49 New Biotechnology (2019) at 100; Andreas Wiebe & Nils Dietrich, Open Data Protection: '*Study on Legal Barriers to Open Data Sharing- Data Protection and PSI'* Universitätsverlag Göttingen, (2017) at 162; Lothar Determan, '*Healthy Data Protection Law*' Michigan Technology Law Review, (2020) at 276.
[155] See Robert Eiss, *'Confusion over Data-privacy Law Stalls Scientific Progress*', Nature (2020).

Within the GDPR, in fact, research plays a crucial role. Recital 157 explicitly declares the Regulation's purpose to facilitate scientific research, a goal that is reflected in the numerous exceptions to the general prohibition on processing special categories of data[156]. These legal justifications are to be combined with the GDPR's specific regulations for research (known as "research exceptions"), among which are the GDPR's Articles 5(1) Lett.b and 6(4)'s default compatibility with the purpose limitation principle on further processing for research purposes.

Recital 159 upholds the broader application of the research exception to private and funded research, avoiding an explicit distinguish distinction between research with advantages to data subjects and the general public. Nevertheless, the same GDPR recital 159 indicates a potential differentiation of data protection regimes, which is echoed in the requirement to take into account "reasons for further measures in the interest of the data subject". In the case of, say, research into rare diseases, it is obvious that this "gives reason for further measures in the interest of the data subject." The recital further states that "in view of those measures, the general provisions of this Regulation should apply." The general rules of the GDPR, however, may be loosened by taking advantage of the Regulation's flexibility when the "interest of the data subject" directly underlying some processing activities is taken into consideration. As a result, while private and public funding for research are not differentiated by the different regimes, the "egoistic" or "altruistic" nature of the research's goals is[157]. The research can be viewed as being in the public interest under the latter hypothesis.

The subjective standpoint regarding the private or public nature of the funding, and consequently the private or public nature of the entities conducting research, appears to be completely irrelevant because it is entirely possible that privately-funded research also serves larger public interest goals, as it can when developing a vaccine during a pandemic.

It is possible to modulate the GDPR's flexibilities differently for research that is profit-driven and public interest-oriented (or altruistic), regardless of the sources of their funding, even under the restrictive approach demanded by the European Data Protection

[156] The numerous exceptions to the general prohibition on processing special categories of data under Article 9(1) GDPR provided by Article 9(2) GDPR include consent (Article 9(2)a GDPR), the need for protection against serious international health threats, the maintenance of high standards for the quality and safety of healthcare, pharmaceuticals, and medical devices (Article 9(2)i GDPR), and the conduct of research activities (Article 9(2)j GDPR). These exclusions must be interpreted in light of the legitimate bases generally established by Article 6(1) of the GDPR.

[157] Giovanni Comandè, Giulia Schneider, '*Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities';* Computer Law & Security Review 41 (2021), at 3.

Supervisor. Such alteration is primarily based on the proportionality and fairness principles, shielding data subjects from the abuses of controllers/processors. According to this viewpoint, the criteria on which the taxonomy is based are the control justifications of the data subjects and the objectives of the free flow of information.

The various interactions between the recalled data protection framework—in particular, the associated exceptions—and the various research goals produce a dynamic spectrum of legal regimes, ranging from full control (for example, through consent) for data processed for profit to data subjects' transfer of control to data controllers for data pools used for non-profit/public interest research-oriented goals. Given the unique characteristics of the research, the data protection exception becomes actually plural: we distinguish between a "data subject-based" regime, a "public interest-based" regime, and a "research-based" regime only.

The rights of data subjects stipulated in Chapter III of the GDPR are fully enforceable under the first regime; under the public interest-based regime, some derogations to those rights may be established by Union or national laws in accordance with article 23 of the GDPR[158]; however, under the research-based regime, significant derogations to those rights are directly contemplated in the GDPR, and additional ones may be introduced by State and Union law in accordance with article 89(2). The GDPR, however, shifts the burden of care onto data controllers who, in order to balance the diminution of actionable data subjects' rights, are required under article 89(1) GDPR to enact adequate safeguards for the protection of data subjects' rights and freedoms:

The decision arising from the Italian Court of Cagliari *Tiziana Life Sciences v. Autorità Garante per la Protezione dei Dati Personali*[159] provides good insights. In order to develop its scientific research activities, in June 2016 Tiziana Life Sciences had acquired from the bankrupt Shar.Dnain liquidation, a company founded in 2000 by Renato Soru, former president of the regional government of Sardinia, the business complex consisting - among others - of genetic data and biological samples extracted from approximately 11,700 individuals. These individuals had voluntarily submitted to samples after being duly informed about the purpose and aims of the research. These individuals are part of a community that has been isolated from the rest of the world for many years and has consequently developed a genetic homogeneity with very few equals: through cross-

[158] See art. 23 (1) lett. e) GDPR specifically referring to public health concerns.
[159] Tribunal of Cagliari, Sentenza n. 1569, 6 June 2017.

referencing studies it is possible to reconstruct common genetic traces in almost all donors, going back as far as 1600. The Garante per la Protezione dei Dati Personali (Italian Data Protection Authority) had intervened by issuing Order No. 389 of 6 October 2016, in which it had imposed the temporary measure of blocking the processing of personal data contained in the so-called biobank for alleged violations of the provisions of the Privacy Code.

In Judgment No. 1569/2017, the Court of Cagliari recognized Tiziana Life Sciences' reasons concerning the unlawfulness of the blocking measure adopted by the Guarantor and ordered the annulment of the measure. Specifically, the Court recognized that it is not necessary to request consent every time the owner of the personal data changes and that the contested measure had not adequately balanced the interests of the parties, imposing on Tiziana Life Sciences an exorbitant measure with respect to the purposes of protecting the subjects involved in the research. In particular, it was shown that the processing of personal data carried out by Tiziana Life Sciences, as the new data controller, pursues the same purposes for which the data subjects had originally given their consent.

We can take from the case that the principles of necessity and proportionality would require processing activities carried out for for-profit research purposes to rely on the legal basis that is more respectful of data subjects' interests and rights: consent and the associated possibility of its withdrawal structurally assures a higher degree of control, even if it is related only to broad research areas, as suggested by recital 33 GDPR (e.g. for data philanthropy, as in the Tiziana case). The presumption of compatibility under articles 6(4) and 5(1) lett. b) GDPR reduces the effectiveness of the data subject's control under consent and allows for further processing for research purposes. However, the aforementioned proportionality and necessity principles impose a strict interpretation of the compatibility rules restricting further flows of research data to data subjects' self-informational determinations (e.g., through notice requirements).

As a result, changing the context (art. 6(4)(f) GDPR) from solely altruistic goals to ones that also include financial gain could result in failing the compatibility test. In addition, Member State laws could not worsen the derogations from basic data protection rights and could be limited to the only ones expressly authorized by the Regulation.

On the other hand, as long as appropriate safeguards are put in place, such as choosing "processing which does not require identification" (art. 11 GDPR), for-profit research can also profit from the deductions. This possibility is directly related to article

89(4) of the GDPR, which establishes the segregation principle and states that privileges are limited to research purposes and do not apply to other purposes.

Different data protection regimes for research have their roots in the GDPR's dual fine-tuning system, which is based on balancing coded data protection principles and rules with the establishment by data controllers of sufficient safeguards for the protection of data subjects' rights and freedoms. From this perspective, the GDPR offers a highly sophisticated regulation of data processing activities for research purposes: it balances research privileges and individual rights privileges, by variously scaling them in relation to the nature of conducted research activities, in order to complement sharing objectives with the high level of protection for data subjects' fundamental rights.

2. Data's monetary value

In order to understand how far-reaching the importance of this "fifth freedom" is, it becomes paramount to try to grasp an understanding of how valueable data actually is in nowadays society. The framework constituted in the GDPR (and all the European Digital Strategy in general), in fact, stems from a recognition from the European Commission that "Data is the lifeblood of economy[160]" and a truly important asset for the future economic and strategic development of the EU market and economy.

While attributing a specific value is quite a difficult task – which many have attempted[161] – given how variable the market is, we can infer from the fact that many companies are willing to forego monetary payment for their digital services in order to gain access to personal data that there is no doubt that it bears a monetary value. This is because, admittedly, the digital industry companies all share one thing, this being the exploitation of the user's personal data through technology in order to acquire a competitive advantage[162]. The significance of data as monetary value is further exemplified by the rise of data-driven

[160] European Commission, *Communication from the Commission. A European strategy for data*. COM(2020) 66 final, 2020) 2.
[161] For an in-depth analysis, *see* Wenfei Fan, Floris Geerts, Jef Wijsen, '*Determining the Currency of Data'*, ACM Transactions on Database Systems, Vol. 37, No. 4, Article 25 (2012).
[162] Guillaume Desjardins, '*Your Personal data is the currency of the digital age'*, La Conversation, (2019).

business models. Companies that have embraced data-centric approaches are disrupting traditional industries, transforming consumer behaviour, and reshaping market dynamics. Sharing economy platforms, for instance, rely on user data to match supply and demand more efficiently, while e-commerce giants employ personalized recommendations to drive customer loyalty and increase sales. Moreover, data serves not only as an economic asset but also as a powerful tool for policymakers and researchers. Governments and organizations use data to gain insights into societal trends, economic patterns, and public health concerns. Data-driven policymaking enables evidence-based decision-making, leading to more effective and efficient public policies and resource allocation.

The outstanding sales volume in advertising can also help us grasp an idea about data's value as the market for targeted advertising online is outstandingly lucrative: according to the annual Interactive Advertising Bureau 2017 IRport, online advertising generated revenues for 88 billion dollars in the United States alone in that year[163], and has raised to 209.7 as of last year [164]. Data's monetary value, however, extends well beyond advertising. In the contemporary digital economy, data-driven insights drive decision-making processes across various sectors. From finance to healthcare and logistics to entertainment, organizations leverage data analytics to optimize their operations, enhance customer experiences, and gain a competitive edge. Data has become a strategic asset that fuels innovation and defines the success of businesses in a rapidly evolving market.

2.1.1. Data as currency in EU, Directive 2019/770

Notwithstanding the sky-rocket high numbers in terms of revenues digital service seem to acquire from the selling of personal data, data subjects appear more than inclined in giving them basically for free, with the only compensation being the access to the digital service. A survey by the Federation of European Data and Marketing shows that 75% of consumers are willing to share data, while 89% acknowledge that businesses are the ones benefiting most from this data exchange[165]. In this sense, personal data becomes the price paid by data subject in order to make the access happen and, in practice, this is not an unfair exchange. In fact, even though we analyzed the hundreds of billions of dollars moved from

[163] IAB internet advertising revenue report of 2017, https://www.iab.com/wp-content/uploads/2017/12/IAB-Internet-Ad-Revenue-Report-Half-Year-2017-REPORT.pdf, .
[164] Advertising Bureau and PricewaterhouseCoopers LLP, IAB internet advertising revenue report, 2022 https://www.iab.com/wp-content/uploads/2023/04/IAB_PwC_Internet_Advertising_Revenue_Report_2022.pdf
[165] DDMA Study: What consumers think about data, https://ddma.nl/kennisbank/consumenten-vinden-dat-bedrijven-meer-profiteren-van-het-delen-van-persoonsgegevens-dan-zijzelf-2016/

data on an yearly basis, it was Clive Humby (who first coined the parallelism of data to oil in 2006) who pointed out how data "is valuable, but if unrefined it cannot really be used[166]."

Nonetheless, the EU, in recognizing this phenomenon, issued the Directive (EU) 2019/770 on contracts for the provision of digital content and digital services[167] which was transposed in Italy through Legislative Decree No. 173/2021[168]. The Directive's goal is to strike the right balance between a high level of consumer protection and the promotion of business competitiveness, ensuring a seamless internal market for goods and services across all of Europe.

Indeed, the variety of national consumer law regulations and, consequently, the costs of adapting their contracts to the specific rules existing in different Member States, pose additional costs for businesses offering digital services across borders, especially SMEs. It is common knowledge that using digital content and services necessitates using the personal data of the user, so the need for regulatory harmonization and the fundamental right that the protection of personal data represents must be balanced. In this regard, the legislative decree, in accordance with the transposed directive, codifies the practice – that is extremely common in the digital sphere – whereby "the trader provides or undertakes to provide digital content or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader"[169]. As a result, the consumer gives up his personal information in exchange for the delivery of digital goods or services; the consumer's accomplishment is to give the trader his personal information, such as name, email, phone number, photo, etc. (Art. 1(4)).

The Directive basically ends up legitimizing the function that we have mentioned to be carried out by personal data, namely serving as "currency" for the purchase of digital goods and services. The similarity with the obligation to pay a price is self-evident, nevertheless it deserves clarification. Unlike the price, the onerous transfer of one's personal data does not allow the consumer to achieve full awareness of the value of his or her data, hence, of the price paid. It does not allow them to understand the scope of the agreement, either in economic terms or in terms of privacy. And so, the phenomenon of data capitalization cannot be said to be complete, in the sense that only the economic operator

[166] Michael Palmer, Clive Humby, '*Data is the new Oil'*, ANA Marketing Maestros, (2006).
[167] 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;* ELI: http://data.europa.eu/eli/dir/2019/770/oj
[168] Decreto Legislativo 4 novembre 2021, n. 173, Attuazione della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. (21G00186).
[169]Directive 2019/770, Art. 1.4.

benefits from it precisely because of this obvious information asymmetry to the detriment of the consumer. Thus, the objective of regulatory harmonization, aimed at protecting consumers and promoting the competitiveness of businesses, has the merit of recognizing legal dignity to such a widespread phenomenon by setting limits and conditions, and will probably help overcome the belief that digital services are free[170].

3. Extent and limits of right to privacy under GDPR

Beyond this economic value, personal data is also intrinsically linked to the dignity, autonomy, and personality of individuals[171]. Moreover, with the increasing value of data[172] comes heightened concerns about data privacy and security. As data becomes an incredibly sought-after commodity, protecting individual privacy and ensuring data security becomes paramount. Striking the right balance between data-driven innovation and robust data protection measures is imperative to build and maintain trust in the digital ecosystem.

This dual nature of personal data is acknowledged, and given expression, in EU data protection policy which seeks to ensure the free flow of personal data while respecting fundamental rights, in particular the rights to privacy and data protection, a legislative framework which is supported by the provisions of the EU Charter of Fundamental Rights. What we argue is that the GDPR operates a good job in fostering the digital single market while protecting the right to privacy of individuals, two seemingly opposite issues, therefore absolving what presents itself as a truly difficult task.

3.1 Privacy by Design and by default

The discipline laid down by GDPR is heavily influenced by the concept of "Privacy by Design", with the same title of Article 25 being 'Data protection by design and by default'. To understand what the concept of Privacy by Design implies, Professor Ann

[170] Gianluca Fasano, '*Dati personali: da «res extra commercium» a moneta di scambio'*, Il Sole 24Ore, (2022).
[171] See European Data Protection Supervisor Opinion 4/2015, Opinion 4/2015, '*Towards a new digital ethics Data, dignity and technology'*, (2015).
[172] See Ignacio Larrú, '*The Rising Value of Data'*, IE Insights, (2018).

Cavoukian (who coined the term) explains how this is built on seven fundamental principles[173], namely:

1) Proactive not reactive; preventative not remedial

Proactive instead of reactive measures define the Privacy by Design (PbD) methodology. It foresees and stops events that would violate privacy before they take place. PbD seeks to prevent privacy risks from occurring rather than waiting for them to manifest or providing solutions to address privacy violations after they have already happened. In other words, Privacy by Design occurs prior to the event, not afterwards. This principle is reflected in GDPR through requirements like data pseudonymization and data breach impact assessments. Before an incident happens, they make sure that organizations and the data they manage are protected and that response plans are established.

2) Privacy as the default settings

Even if a person does nothing, their privacy is still protected. The system is designed to protect privacy by default, so an individual doesn't need to take any action to do so. The way businesses ran permission pass campaigns and created their cookie consent banners was influenced by this idea. It should have been assumed that if a recipient did not reply to the email requesting their consent to contact them again in the future. Furthermore, non-essential tracking cookies would be disabled by default, necessitating user consent rather than allowing users to reject them.

3) Privacy embedded into design

IT systems and business practices are created with privacy by design ingrained into the design and architecture. It is not an after-the-fact addition that is bolted on. As a result, privacy is made a fundamental part of the core functionality being provided. The system incorporates privacy without sacrificing functionality.

4) Full Functionality — Positive-Sum, not Zero-Sum

With Privacy by Design, no unnecessary trade-offs are made and all legitimate interests and goals are accommodated in a positive-sum "win-win" way rather than the outmoded zero-sum method. By demonstrating that it is possible to have both privacy and security, Privacy by Design does away with the pretence of false dichotomies like privacy vs. security.

[173] Ann Cavoukian '*The 7 Foundational Principles'*, (2011) PbD available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

5) End-to-end security – full lifecycle protection

Full lifecycle protection for personal data entails safeguarding the data both while it is at rest and in motion (Article 32), retaining it only as long as it is necessary (Article 25), and deleting it when the data subject requests it (Article 17).

6) Visibility and Transparency — Keep it Open

Privacy by Design aims to reassure all stakeholders that, subject to independent verification, whatever the business practice or technology involved is actually operating in accordance with the stated promises and objectives. Both users and providers can still see and understand how it works and its component parts. In this direction, many businesses updated their privacy policies to be GDPR compliant in the interest of visibility and transparency. These updates included, among other things, thorough lists of all tracking cookies that specify the cookies' origin, the information they gather, how long the information is stored, and the purposes for which it is used.

7. Respect for user privacy – keep it user-centric

All the aforementioned ideas serve as the cornerstone of user-centricity, which is essential to protecting data subjects' rights and maintaining their privacy. Architects and operators are required by Privacy by Design to prioritize the needs of the individual over all else by providing features like strong privacy defaults, appropriate notice, and empowering user-friendly options.

As we have seen, all the foundation principles underlying the concept of Privacy by Design concur – at least in principle – to foster a better, more secure, and privacy-conscious digital landscape. By taking a proactive, user-centric approach to data protection, Privacy by Design ensures that privacy considerations are integrated from the outset of data processing activities, making the – admittedly non-negligible – effort to comply with the data protection framework a great way to gain the necessary trust from users. Moreover, Privacy by Design aligns perfectly with the pivotal role played by consent in the GDPR, as both principles prioritize individual empowerment and control over their personal data. By putting privacy at the forefront of data processing activities and respecting the rights and choices of individuals, organizations can build a trustworthy and responsible data-driven ecosystem within the Europea nmarket. Nevertheless, GDPR general requirements do not stop here,

bringing along numerous other rights of the user of which controllers and processors must be aware of and most of all compliant to[174].

4. Privacy first… and issues with it. Meta Platforms Inc. v. Bundeskartellamt and TikTok

As anticipated, notwithstanding the concerns raised by privacy advocates regarding the perceived generality of the GDPR's provisions, our analysis aims at demonstrating the importance of considering the regulation's dual objectives. In order to design privacy regulation, policymakers must balance consumer privacy concerns with the benefits of the data economy[175]: if privacy regulation harms competition, for instance, this compound concerns about market power in the economy[176]. On the other hand, if one of the two interests appears to prevail on the other, in recent years this has been definitely the privacy of the users. The judges of Luxembourg appear, in fact, to become more and more strict on the application of the provisions of the Regulation and while this should make the said privacy advocates feel safer, this trend do not come without risks.

The Court's decision in *Meta v. Bundeskartellamt*[177], and the discussion it triggered, provides much food for thought on the topic. While the case is not alone in showing the court's inclination not to overlook the right to privacy when it comes to economic concerns[178], it clearly showcases the intricate tension between market functionality and privacy, focusing on user consent and data processing practices.

---

[174] Namely: Right to be informed - Notify users about how you obtain and process their data in a brief, intelligible, and easily accessible form; Right of access - Allow users to obtain information about how you use, store, or disclose their data; Right of rectification - Let users correct inaccurate information about them displayed in your records; Right to erasure - Promptly delete users' data at their request; Right to restrict processing - Stop processing users' data at their request; Right to data portability - Allow users to transfer a copy of their data to another company; Right to object - In certain instances, users can object to the processing of their personal data; Rights related to automated decisions - Protect users from automated decisions by granting a review when requested.

[175] *See* Garrett A. Johnson, Scott K. Shriver, Samuel G. Goldberg *'Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR'*, Management Science, (2023) at 2.

[176] Council of Economic Advisers (2016) Economic report of the President. Technical report, Council of Economic Advisers, Washington, DC ; see also Steven Berry, Martin Gaynor, Fiona Scott Morton '*Do increasing markups matter? Lessons from empirical industrial organization'*. Journal of Economic Perspective 33(3), (2019) at 45.

[177] Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt*, ECLI:EU:C:2023:537.

[178] *Inter alia*, CJEU, Case C-131/12, Google Spain, 13 May 2014; Case C-293/12, Digital Rights Ireland and others, 8 April 2014; Case C-498/16, Schrems I, 25 January 2018; Case C-311/18, Schrems II, 16 July 2020. See also: Oreste Pollicino, *Judicial protection of fundamental rights on the Internet: A road towards digital constitutionalism?*, Hart Publishing (2021).

Within the EU, Meta Platforms Ireland (Meta), responsible for services such as Facebook, Instagram, and WhatsApp, relies on a business model of personalized advertising, creating comprehensive user profiles from both direct and indirect ("off-Facebook") data. Through the aggregation of this data, Meta can infer user preferences and interests, a process governed by a user agreement that requires consent to Meta's terms. The Federal Cartel Office (Bundeskartellamt) in Germany took legal action against Meta Platforms, including Facebook Deutschland and Meta Platforms Ireland, challenging the conditions under which "off-Facebook data" was processed without explicit user consent. In response, the Bundeskartellamt's decision prohibited the companies from conditioning the use of Facebook on such data processing for private users in Germany, and from doing so without their consent. The companies subsequently filed a lawsuit against the ruling with the Düsseldorf Higher Regional Court, which then sought a preliminary ruling from the CJEU, Europe's highest court.

4.1.1. How to collect data? Luxembourg tightens the requirements

In its decision the CJEU defines the conditions for the operator of an online social network to lawfully process Social Network Data by strictly interpreting the legal justifications of Article 6(1) GDPR. First of all, the Court aligns with the Advocate General's conclusion[179] for which Article 9(1) GDPR's general prohibition against processing special categories of personal data applies regardless of whether the information revealed by the processing operation in question is accurate and regardless of whether the controller is acting with the intention of obtaining information that is related to one of the special categories mentioned in that provision. Instead, the prohibition must apply regardless of the processing's declared purpose (paragraphs 69 and subsequent). Thus, the argument over whether these requirements restrict the applicability of Article 9(1) GDPR is resolved. The CJEU further maintains that when users of a social network visit websites or apps and use integrated buttons, like the "Like" or "Share" buttons, that may reveal information falling under one or more of the special categories of personal data referred to in Article 9(1) GDPR, Meta processes sensitive personal data in the sense of that provision. By doing this, users provide information to these websites or apps, and Meta uses that information by connecting it to the user's social network account [180]. Neverthelesss, the CJEU ruled that "it cannot be

[179] Case C-252/21, Meta Platforms, Inc. v. Bundeskartellamt, Opinion of AG Rantos of 20 September 2022, ECLI:EU:C:2022:704.
[180] *Meta Platforms Inc and Others v Bundeskartellamt*, para. 71 et seq.

inferred from the mere visit to such websites or apps by a user that the personal data in question were manifestly made public by that user within the meaning of Article 9(1)(e) GDPR"[181]. Depending on the personal preferences a user selects, the degree to which an interaction with such a website or app is considered public may change. According to the CJEU, the exemption of Article 9(2)(e) GDPR will only be applicable if users have the option to make the information accessible to the general public or, instead, to a more or less limited number of selected persons based on settings chosen and with full knowledge of the facts (paras 80 et seq.)

Most importantly, the Court emphasizes that to consider personal data processing as "necessary" for the performance of a contract, it must be "objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject," tightening the requirements for basing such processing on social network data under Article 6(1)(b) GDPR. The controller must demonstrate how, without said processing, the primary goal of the contract cannot be achieved. According to the judgment, "the mere fact that such processing may be mentioned in the contract or may merely be necessary for its performance is, in and of itself, irrelevant in that regard [182]".

While acknowledging that users gain from personalized content as it enables viewing material corresponding to their interests, the Court notes that personalized content does not seem required to provide online social network services. It adds that "those services may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalization, such that the latter is not objectively indispensable for a purpose that is integral to those services"[183]. Consequently, the judgment concludes that the processing of personal data from services unrelated to Facebook within Meta's offerings does not appear necessary for delivering the Facebook service.

Furthermore, the Court adopts a similarly constrained interpretation of Facebook's legitimate interests in processing users' Social Network Data, relating to the legal justification under Article 6(1)(f) GDPR. In evaluating Facebook's legitimate interest, the Court emphasizes that "the interests and fundamental rights of the data subject may, in particular, override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing" (para. 112; cf. recital 47 GDPR). While recognizing Facebook's general legitimate interest in personalizing

[181] Ibid, para. 79.
[182] *Ibid* para. 98.
[183] *Ibid* para. 102.

content, the Court underscores that controllers wishing to rely on this legal basis must adhere to stringent guidelines. Specifically, processing is confined to what is "strictly necessary for the purposes of that legitimate interest".

Finally, even though Facebook's services are free, the CJEU notes that users "cannot reasonably expect that the operator of the social network will process that user's personal data, without that user's or his or her consent, for purposes of personalized advertising." Therefore, in those circumstances, the CJEU ruled that the interests and fundamental rights of such a user outweigh Facebook's interest in the type of personalized advertising that allows it to support its operations (para. 117).

4.1.2. Consent from users is non-negotiable in the GDPR, TikTok case

The judgement of the CJEU marks a turning point in the larger discussion on the legal justifications for the collection and use of personal information for advertising and microtargeting on digital platforms. The debate peaked when in June 2022, TikTok announced changes to its terms and conditions regarding privacy and data protection policies in the European Economic Area, the United Kingdom, and Switzerland. According to the announcement, as of July 2022, its legal basis under the GDPR would change from reliance on consent to legitimate interests[184]. In particular, "information that businesses share with us in order to reach potential customers on TikTok" was among the data that was deemed to have been used by users for both their on- and off-TikTok activity. Widespread criticism and questions about whether TikTok's decision was compliant with the GDPR were raised in response to this ambiguous change in the terms and conditions[185].

The main concern was the legality of basing data processing for advertising purposes on legitimate interest rather than consent, especially in light of the CJEU's Fashion ID ruling and the EDPB's updated Guidelines 8/2020 on the targeting of social media as of April 2021. First of all, it has been noted that it is unclear why TikTok chose to rely on the legal justification of legitimate interests with respect to the data provided by users when using the social network should be acknowledged as necessary for the platform and proportionate to the pursuit of its business interests. Second, it has been made clear that, contrary to the EDPB's recommendations, it is difficult and counter-intuitive for users to exercise their right

[184] TikTok Newsroom, https://newsroom.tiktok.com/en-eu/changes-personalised-ads-eu.

[185] See *inter alia*, Euroconsumers, '*TikTok's new policy of advertising must be stopped'*, (2023) available at https://www.euroconsumers.org/opinions/tiktoks-new- policy-of-advertising-without-consent-must-stop; Access Now, '*Immediately no: TikTok's new personalised ads will jeopardise rights in Europe'*, available at https://www.accessnow.org/press-release/immediately-no-tiktoks-personalised-ads-europe/ (2023).

to object to the processing of their personal data before the processing itself is started. Third, Article 5(3) of the Directive 2002/58/EC (e-privacy Directive) requires the need for free and informed consent - to the extent this is based on cookies or other information stored on the user's device - so that legitimate interest, in the words of the EDPB, does not represent the appropriate legal basis with respect to observed data (i.e., data that is not actively made available to the social media provider but that is provided via the simple use of the platform).

The Italian Data Protection Authority issued a decision[186] in July 2022 alerting the social network to the likelihood that this action would violate both the GDPR and the national laws implementing the e-Privacy Directive. In actuality, the processing of user data obtained from their personal devices for advertising purposes without their consent would be prohibited by the Italian DPA. Additionally, the decision found that the new policy would probably affect both minors and adults due to the challenges TikTok admittedly faced in implementing age verification methods. The Italian DPA's decision, moreover, was not the only one. The Irish and Spanish Authorities also swiftly intervened to warn TikTok, which led to the platform's ultimate decision[187] to suspend the adoption of the new privacy policies shifting the legal basis from consent to legitimate interest.

4.1.3. Privacy conquest, market concern or…both

Both the cases of Meta and TikTok demonstrate the importance of privacy and data protection rights within the EU's legal system. In fact, over the past ten years, there has been a sharp rise in the number of concerns held by European and Member State institutions, from the European Court of Justice to the European Parliament and the Commission to domestic authorities, which has resulted in the construction of a European fortress of personal data[188] and raised concerns about the viability of the business models of online platforms.

Even though the protection of constitutional values, particularly fundamental rights, serves as the foundation for these worries and the institutional responses to them, the

[186] Provvedimento del 7 luglio 2022 [9788429], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9788429

[187] https://edpb.europa.eu/news/news/2022/edpb- adopts-letters-access-now-and-beuc-tiktok-and-art-65- dispute-resolution-binding. In an update to its decision of July 12, 2022, TikTok declared: "While we engage on the questions from stakeholders about our proposed personalised advertising changes in Europe, we are pausing the introduction of that part of our privacy policy update. We believe that personalised advertising provides the best in-app experience for our community and brings us in line with industry practices, and we look forward to engaging with stakeholders and addressing the concerns".

[188] Oreste Pollicino, Pietro Dunn, '*The Sustainability of European Privacy and Data Protection'*, MediaLaws, Law and Policy of the Media in a Comparative Perspective (2022).

approach taken by Europe in this area raises serious concerns about the long-term economic and technological viability of the European data protection legal framework[189].

Following such an absolute approach runs the risk of resulting in an overly restrictive enforcement, which would ignore the crucial function of balancing in European constitutionalism. A disproportionate enforcement may ultimately affect that balancing act if the business model of social media platforms like TikTok is based on the promotion of advertising, which is typically personalized and customized based on users' interests and preferences.

Before GDPR came into force, the vice-president of the giants of telecommunication Ericsson's Ulf Pehrsson duly warned[190] EU policymakers to avoid the three common major mistakes, that is worth emphasizing. The first is a rhetorical one, as the frequently argument used by policymakers is that increasing privacy regulations will boost business competitiveness, claims that are not supported by experience or economic theory, however, and no compelling evidence has yet been offered to support them. Attitude comes in second, as businesses that raise objections to privacy proposals are frequently dismissed and accused of violating the fundamental right to privacy, all that it accomplishes is maintaining a biased policy approach and prevent the emergence of constructive, balanced, and progressive privacy policy legislation. Finally, substance is the third, with a call for DG Justice, the European Data Protection Supervisor, and future data protection authorities to all take into account Europe's need for better and more intelligent regulation. The hope lies in a more market oriented approach from the Court, as the framework depicted in the Regulation appears to be driving towards the good direction An example is provided by the discipline on Automated Decision Making.

4.2 GDPR to the test: ADM

In addressing profiling first, GDPR defines it at Art. 4(4) as an automated form of processing, which is carried out on personal data and its objective is to evaluate personal aspects about the data subject. Its relevance to our reasoning relies on the fact that profiling is often the first step in automated decision making for which, on the other hand, the

[189] *Ibid.*
[190] See '*Europe's obsession with privacy rights hinders growth'*, opinion by Ulf Pehrsson, (2016), https://www.politico.eu/article/opinion-europes-obsession-with-privacy-rights-hinders-growth/

Regulation doesn't provide an express definition. It is Article 22 that takes into account both the activities[191], stating 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*"[192]. The wording of such article has created heated debates as it admittedly leaves significant room for interpretation on many aspects. Completing the GDPR, Article 29 Working Party[193] provides some much-needed clarifications. In addressing one of the most important issues, it firmly states that Article 22 of the GDPR – despite the wording which would induce to think otherwise – does not grant a right on data subjects but establishes a general prohibition on solely automated individual decision-making, applied whether or not the data subject takes any action in response to such processing. This interpretation itself wasn't unscathed by critics: while aiming at strengthening individuals' control over their data, on the other hand this "prohibition masked as a right"[194] ends up diminishing legal certainty for both the data subject and controller[195]. In truth, the GDPR admittedly introduces several individual notice and access rights related to automated decision-making in addition to Article 22. When information is obtained directly from users, Article 13 stipulates a number of notification rights and obligations[196]. Similar ones are established by Article 14 when personal data about individuals is obtained from third parties[197] while Article 15 grants an individual right to access information stored by a company that may be solicited "at reasonable intervals"[198].

Furthermore, the second paragraph of article 22 provides for only three cases in which the prohibition previously mentioned doesn't apply, namely: a) solely automated decision making is necessary for entering into/performance of a contract between the data subject and a data controller; b) it is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; c) is based on the data subject's explicit consent . These exceptions caused a sensation among scholars as well, triggering

[191] GDPR, Art. 22.
[192] *Ibid.*
[193] Article 29 Working Party.
[194] Mariam Hawath, '*Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR'*, European Data Protection Law Review 161 (2021), at 164.
[195] In this Sense, Aleksandra Drożdż, '*Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR*', European Monographs 113 (2019), at 38.
[196] Art 13 GDPR.
[197] *Ibid*, at art 14.
[198] *Ibid*, at art 15.

skepticism around the effectiveness[199] of the discipline in both constraining ADM and protecting data subjects, as the contract and consent derogations may in fact lessen the protection granted by the prohibition of art 22(1). The common opinion is that informational and power asymmetries between the data subject and controller are too wide to empower individuals against opaque and complex systems, with privacy notices used to gather consent for automated decision-making often requiring an advanced tech-law knowledge which obviously the average data subject lacks.

Nevertheless, as we navigate the dynamic landscape of data-driven technologies a layer deeper from a privacy safeguarding perspective, it becomes evident that Automated Decision-Making Systems present both challenges and opportunities in the context of data protection under the GDPR, as the automation agenda is mostly one of cost savings and efficiency[200]. While depicted as a shady evil to avoid, with the scholarly example being the computer of the bank denying a loan to the poor citizen, it seems to be forgotten how ADMS when wisely used enhance efficiency, improve services, and drive innovation in various industries.

For small, medium and even large businesses, activities such as targeted digital and mobile advertising has become a crucial tool in attracting customers and surviving challenging times[201]. For example, many online journals and news websites provide free access to their content to attract readers. However, to sustain their operations and maintain a revenue stream, these platforms rely on advertising and personalized content recommendations. This is where ADMS come into play. When users visit an online journal or news platform, ADMS are employed to process data about their browsing behaviour, interests, and preferences. By analyzing this data, the system can deliver targeted advertisements and personalized content suggestions to individual users. This level of personalization enhances the user experience, increases engagement, and optimizes ad revenue for the platform, which are vital to this day, with journals all over Europe starting to present the user an aut-aut: either accepting cookies or paying the subscription, which steadily drives into the direction of personal data used as a digital currency of which we

[199] *Inter alia*, see 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'*, International Data Privacy Law, Vol. 7, No. 2 (2017); Celine Castets-Renard, '*Accountability of Algorithms in the GDPR and beyond: AEuropean Legal Framework on Automated Decision-Making'*, The Fordham Intellectual Property, Media and Entertainment Law Journal. 91 (2019).
[200] In this sense, see Malcolm Langford, *'Taming the Digital Leviathan: Automated Decision-Making and International Human* Rights' American Journal of International Law - Unbound, Vol. 114 *(*2020*)* at 146, referring to the Report of the Special Rapporteur on Extreme Poverty and Human Rights, UN Doc. A/74/48037, para. 8 (2019).
[201] Lisa Lottering, '*Balancing Privacy and Digital Marketing in the Information Age'*, (2021), CM Blog, available at https://www.cm.com/en-za/blog/balancing-privacy-and-digital-marketing-in-the-information-age/

discussed briefly above. Moreover, as it has been noted[202],marketers and marketing agencies who gather and use personal data for individualized advertising and marketing campaigns may be considered performing "profiling" under the GDPR at best. Such organizations will want to make sure their use of profiling is justified and that they adhere to the GDPR's transparency and other data protection requirements. Moreover, as we have seen, under the Regulation fully "automated decision-making" is generally forbidden, this implying that the majority of decisions made by marketers and marketing organizations may not involve individuals' contractual or legal rights, legal status, or other important types of rights, so it is possible that they are not engaging in such "automated decision-making" in the first place and in any case the GDPR will require compliance with one of the justification above to support it if a marketer or marketing organization wants to perform such fully automated decision-making.

In sum, ADMS are both difficult to happen under the Regulation and well constrained if performed. Clearly, with the implementation of ADMS comes the responsibility to respect users' privacy but GDPR's principles of data protection by design and by default are fundamental in addressing these intricacies of ADMS. Privacy by Design encourages organizations to integrate privacy considerations into the development of ADMS from the outset. This approach ensures that data protection measures are embedded into the core functionalities of these systems, promoting responsible data practices and safeguarding individuals' rights.

Transparency also emerges as a critical aspect in the intersection between ADMS and the GDPR. Article 22 of the GDPR specifically addresses the right to explanation for individuals subject to automated decisions, granting data subjects the ability to obtain meaningful information about the logic, significance, and potential consequences of automated processing. Transparency in ADMS helps individuals understand how their data is used and how decisions that affect them are made, fostering trust and accountability.

Finally, as ADMS evolve and become more sophisticated, the GDPR's data protection impact assessment (DPIA) requirement gains significance. The Regulation’s obligation enshrined at Article 35, in fact, imposes organisations to conduct DPIAs to identify and assess the potential risks posed by ADMS to individuals' rights and freedoms when the treatment specifically calls for the use of new technologies. This proactive

[202] *See* ReedSmith, ‘*Advertising and the GDPR’s Requirements on Automated Decision-Making and Profiling’,* Association of National Advertisers, at 4-5.

assessment enables controllers to implement necessary measures to mitigate risks and ensure compliance with the GDPR's principles.

In conclusion, the interplay between ADMS and the GDPR is intricate, but the regulation's principles provide a solid foundation for addressing the challenges posed by these data-driven technologies. By promoting transparency, accountability, and user-centricity, the GDPR fosters a data-driven economy that respects individuals' privacy rights while encouraging responsible innovation within the EU internal market. The GDPR's balanced approach seeks to maximize the benefits of ADMS while upholding the fundamental principles of data protection, reflecting the regulation's commitment to protecting individuals' rights in the digital age.

5. GDPR and Data transfer

Shifting the focus on the Regulation's discipline on data transfer, cross-border data flows have been referred to as "the connective tissue holding the global economy together[203]" as well as "hallmarks of 21st century globalization"[204]. According to one estimate, cross-border data flows increased the global GDP by $2.8 trillion in 2014 Both in terms of the volume of data flows and their monetary value, the importance of international data trade has only been increasing. Nevertheless, as this aspect of globalization evolved, countries did not harmonize their data privacy laws, growing a number of distinct governance models that were adopted to chase own strategic benefits.

GDPR regulates the extraterritorial application of data privacy in Europe, while in the US this is a matter of state legislation. The Regulation provides protection for natural persons "whatever their nationality or place of residence" with regard to the processing of their personal data. The discipline, which is contained in Chapter V of the regulation under consideration, substantially reproduces the guiding principles of Directive 95/46

[203] McKinsey Global Institute, '*Globalization in transition: the future of trade and value chains'* (2019) , available at https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains

[204] McKinsey Global Institute, *'Digital globalization: the new era of global flows'* (2016), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

constituting, however, an evolution and an improvement, both in quantitative and qualitative terms.

In particular, Article 45 provides for three mechanisms through which it is possible to implement the transmission of personal information between the EU and third States. The first of these is the adequacy decision, whereby the European Commission, following the overall assessment of a series of elements concerning the legal system of a third country, agrees that that country is able to provide an 'adequate level of protection' for personal data[205] ; in other words, it is such as to ensure, in law and in fact, protection equivalent to that provided for in the EU[206].

In the absence of an adequacy decision, the second mechanism for transferring personal information to a non-EU country, enshrined in the GDPR, is based on "adequate safeguards". More precisely, in this case, the data controller or processor may authorize the transmission of data to a third country, provided that this transmission is accompanied by adequate safeguards and that data subjects are granted enforceable rights and effective remedies[207]. Both Standard Contractual Clauses and Binding Corporate Rules[208] may constitute such safeguards. The former are clauses drawn up on the basis of certain Commission decisions[209] and agreed upon between the data exporter (established within the EU) and the data importer (operating outside the EU) which are included within a given contract. These clauses produce binding legal effects between the contracting parties, imposing, in particular, detailed protection obligations on the importer of data that carries out its activities in a third country. Binding Corporate Rules, on the other hand, are rules that multinational companies adopt internally, which, by binding all companies belonging to the same group, allow the flow of data to foreign subsidiaries located outside the EU. The transfer of personal information under this mechanism is subject, in the absence of the consent of the data subject, to the prior authorization of a national supervisory authority.

---

[205] GDPR, Art. 45(1)(2).

[206] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI identifier: ECLI:EU:C:2015:650 paras. 73-74; on the notion of equivalent protection, see: G. Maldoff, O. Tene, '*Essential Equivalence' and European Adequacy After Schrems'*: The Canadian Example", Wisconsin International Law Journal, Forthcoming, (2017)

[207] GDPR, art 46 (1).

[208] GDPR, Art. 46(2)(3); On this profile, see: Christopher Kuner, *'Reality and Illusion in EU Data Transfer Regulation Post Schrems'*, German Law Journal 881, (2017) at 906.

[209] These are, in particular, four decisions: Commission Decision No. 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC; Commission Decision No. 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC; Commission Decision No. 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; Commission Decision No 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

Finally, the third and final form of extra-EU data transmission is the one based on the requirement for exemptions laid down in Article 49 of the GDPR, which, based mainly on the consent of the data subject, allow such transmission, even in the absence of an adequacy decision and adequate safeguards[210].

5.1.1. The notion of establishment under Data Privacy Law

Article 3[211] gives away the Regulation's expansive territorial scope maintaining how this will be applicable to all processing of personal data "in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not." The Recitals provide some needed guidance as to the definition of "establishment" (given that the GDPR solely defines the term "main establishment"[212]), indicating "the effective and real exercise of activity through stable arrangements"[213]. This has been further interpreted by scholars as referring to the place where the controller conducts the "effective and real excerice of activities" while having human and technical resources necessary to achieve certain services through "stable arrengements" [214]

The section of this provision requiring a determination of whether or not an establishment in the EU is involved may also be interpreted in light of case law from the Court of Justice of the European Union ("CJEU"), even if that case law was issued under the 1995 Directive, which was the GDPR's forerunner. But a case-by-case examination is required to establish whether the processing is carried out in connection with the operations of such an establishment or not[215]. Previously analyzed case Google Spain provides a good

[210] GDPR, Art. 49.
[211] GDPR, Art. 3
[212] *Ibid*. art. 4(16) (for a controller with establishments in more than one EU Member State, "the place of its central administration in the Union, unless the decisions and the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment").
[213] *Ibid*, Recital 22, which adds "The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."
[214] See Gregory Voss, Katherine Woodcock, '*Navigating EU privacy and data protection laws',* ABA Section of International Law (2016), at 32 (Voss and Woodcock were referring to the 1995 Directive, the same meaning applies to term "establishment" as used in the GDPR).
[215] See Dan Jerker B. Svantesson, '*Article 3 Territorialscope'*, in the *'EU General Data Protection Regulation(GDPR): a commentary'* in The EU General Data Protection Regulation (GDPR): A Commentary Christopher Kuner et al. eds., (2020) at 87. The EPDB has also provided examples analyzing different cases under Article 3(1). *See* Guidelines3/2018 on the Territorial Scope of the GDPR (Article 3). https://edpb.europa.eu/sites/edpb/Files/files/filel/edpbguidelines32018_teritorialscopeafterpublic consultation en 1.pdf [hereinafter Guidelines 3/2018].

example: because the activities of its Spanish establishment, including the advertising, assisted in financing the U.S. company's search engine, the court further determined that the U.S. company was subject to the DPD. Nevertheless, the case which sorted every doubt was *Weltimmo*[216].

5.1.2. Weltimmo to clarify establishment requirements for online services and DPAs powers

Weltimmo, the applicant, is a Slovakian (as it is registered there, but without carrying any activity) company without a registered office or branch in Hungary but runs a website regarding Hungarian properties in the Hungarian language and that process the personal data of the advertisers. For the first month, the advertisements are free but, after that, a fee is due. Following the one-month period, many advertisers sent emails requesting the removal of their advertisements and personal information. In refusing to delete the data, the applicant proceeded to charge the interested parties. In addition to charging the interested parties for its services, the applicant refused to delete the data. Furthermore, since these sums were not paid, the applicant forwarded the advertisers' personal information to debt collection companies. Therefore, advertisers complained to the Hungarian Data Protection Authority ("DPA"), which investigated the matter and issued a fine of 10 million HuF (32.000 EUR approximately) against Weltimmo. The Slovakian company contested the fine with the Hungarian Court, claiming that the DPD did not apply to them on account of several factors. Namely, it did not have a branch or office in Hungary; it was not established in Hungary and did not meet any of the other criteria for the application of Hungarian law under the Directive. The issue was then referred by the Hungarian courts to the CJEU.

The Court maintained that Weltimmo had to be considered as a Hungarian company, and this for a number of reasons: first, the online service they ran in the Hungarian language concerned Hungarian properties. Moreover, and most importantly, the debt collectors instructed by Weltimmo used a postal address in Hungary and possessed a Hungarian account to do business on Weltimmo's behalf, acting as its "representative". The mere presence of a single representative in the Member State for the Court is sufficient to create an establishment of the controller on its territory and, for all these reasons, Weltimmo was deemed subject to Hungarian law, while the nationality of the advertisers (in this case data subjects) were considered as irrelevant. The European Data Protection Board ("EDPB") in

[216] Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*,; ECLI:EU:C:2015:639.

summarizing the CJEU's ruling, stated "that the notion of establishment extends to any real and effective activity-even a minimal one-exercised through stable arrangements" where the threshold for "stable arrangements" is quite low[217].

The judgement bears serious practical consequences, recognized by scholars to have the "potential to significantly impact the way in which global organizations should be thinking about their data protection strategy in Europe"[218]. The case dealt with both the rules determining which national data protection law applies to an organization that is operating in multiple EU member states and the powers of national data protection authorities (DPAs) in such cases.

As to the former, it clarifies that the concept of establishment must be interpreted broadly with the legal form of such establishment (e.g. branch, subsidiary etc) not constituting the determining factor (leaving no space for the formalist approach whereby organizations are considered to be established solely in the place in which they are registered). Nevertheless, there is no "bright line" Weltimmo-test stemming from the judgement, with the CJEU preferring to rely on a broad range of factors in order to make a finding on a case-by-case basis[219]

Furthermore, *Weltimmo* provides some much-needed clarifications on Data Protection Authorities (DPAs) and their powers. If a DPA determines that a company has an establishment in another Member State, it may, in accordance with Article 28(4), only use its powers granted by Article 28(3) within its own territory and may, without first determining which national law is applicable, conduct an investigation into the complaint. Nevertheless, that DPA cannot impose penalties outside of its own Member State's borders when and if it becomes evident that the law of another Member State applies.

In being groundbreaking, *Weltimmo* didn't attract as much attention as it did the case of which it followed suit (*Google Spain*), having been mostly overshadowed by the decision in *Schrems* [220] issued only few days afterwards. The Schrems saga marked a turning point in

---

[217] See Gregory Voss, '*Cross-Border Data Flows, the GDPR, and Data Governance'*, Washington International Law Jorunal Vol. 29 No.3 (2020), at 497.

[218] Golden data Law, '*Weltimmo and the concept of 'establishment' under EU Data Protection Law'*, (2019) available at https://medium.com/golden-data/weltimmo-and-the-concept-of-establishment-under-eu-data-protection-law-1b48fb78938d.

[219] Hunton Andrews Kurth, *'CJEU Applies Broad Territorial Scope to EU Data Protection Law'*, Hunton Privacy Blog (2015) available at https://www.huntonprivacyblog.com/2015/10/05/cjeu-applies-broad-territorial-scope-to-eu-data-protection-law/.

[220] *See* Golden data Law, '*Weltimmo and the concept of 'establishment' under EU Data Protection Law'*, and Dennis Kelleher, '*You're Watching Schrems, but Maybe You Should Be Watching Weltimmo'*, IAPP (2015) available at https://iapp.org/news/a/youre-watching-schrems-but-maybe-you-should-be-watching-weltimmo/.

the realm of data protection and had profound implications for data transfers between the EU and third countries.

5.2 Data transfer issues and the Schrems Saga

5.2.1. Introductive remarks and Schrems I

The constant flow of data across jurisdictions inevitably brings issues regarding conflicting laws and the protection of rights with it. The Schrems saga mainly revolves around the issue of the compatibility of US privacy and electronic surveillance legislation within the EU law. In the following section, we will delve into the anlaysis of the case and its implications, beginning by individuating the grounds of this incompatibility which lies in the inherent differences between the US/4th amendment approach and the EU/GDPR one. On the one hand, the GDPR - which has taken up, developed and perfected the inspiring principles of the processing and transfer of personal information, originally laid down by Directive 95/46 of 1995 - has given rise to the creation of a complex and articulated regime aimed at a real protection of individual privacy[221]. On the other hand, the US legal system does not adequately guarantee the protection of the right to privacy, considering it easily derogable for public security purposes[222]. In this regard, it should be noted that, while on the Fourth Amendment[223] to the US Constitution expressly safeguards this right from ex interference from the executive, on the other hand, it has a significant loophole, being applicable to US citizens only. This situation gets all the more complex and delicate in the light of the wide-ranging powers of control and supervision of personal information granted

[221] Michele Nino, '*La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo'*, Diritti umani e diritto internazionale, Vol.14 Fascicolo 3 (2020) at 735.

[222] Sherri J. Deckelboim, '*Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU–US Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses'*, Georgetown Journal of International Law Vol.48 No.1 (2016), at 272; Gert Vermeulen, '*Eyes Wide Shut: The Privacy Shield's Blunt Denial of Continued Bulk, Mass or Indiscriminate Collection or Processing and Unnecessary or Disproportionate Access and Use by US Intelligence and Law Enforcement Authorities*', in Data Protection and Privacy Under Pressure. Transatlantic Tensions, EU Surveillance, and Big Data, (2017), at 49.

[223] Fourth Amendment to the Constitution of the United States of America, 17 September 1787.

to intelligence and police authorities in preventing and combating organised crime and international terrorism[224].

The obvious structural divergences that exist between the European and US legal systems, with regard to the protection of privacy and personal information, have led the US and EU authorities to find compromise solutions in recent years, aimed at admitting the flow of data between the two sides of the Atlantic in spite of everything.

As well known, in 2000 the EU and the United States, with the aim of facilitating their trade relations, set up the Safe Harbour system, which was centred on the voluntary adherence to certain European principles on the protection of personal information by American companies operating in Europe, and on the control of this adherence entrusted to two bodies of the US administration (the Federal Trade Commission and the Department of Transportation). This system represented the main instrument of data transfer between the US and the EU, until 2013, when the international press highlighted the Datagate scandal, i.e. the implementation of the PRISM programme by the US authorities, aimed at the generalized storage of European citizens' personal information (also known as Snowden scandal, thanks to the agent who brought up the revelations). This scandal cast serious doubts on the legitimacy of such a system, in light of the circumstance that all the US companies that were involved in the programme and allowed these authorities access to data stored and processed in the US had self-certified their adherence to the Safe Harbour principles[225]. As a result, the EU Court of Justice, in its well-known *Schrems I*[226] judgment of 2015, declared the Safe Harbour regime invalid, finding it incompatible with the relevant data protection and privacy legislation[227].

The following year in July 2016, the European Commission and the United States adopted the EU-US Privacy Shield[228] which, replacing the old Safe Harbour system, became

[224] On this aspect, see Giorgio Resta, '*La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE'*, Il diritto dell'informazione e dell'informatica, Vol. 31, No. 4-5 (2015), at 697.
[225] Communication from the Commission to the European Parliament and the Council on the functioning of the 'Safe Harbour' regime from the perspective of EU citizens and companies established there, COM(2013)847 final, 27 (2013), at 17.
[226] *Schrems v Data Protection Commissioner* (Schrems I).
[227] *Ibid*. For an in-depth focus see Marina Škrinjar Vidović, '*Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities'*, Croatian Yearbook of European Law and Policy Vol. 11 No.1, (2015), 259–275.
[228] The shield consisted of a series of annexes: Annex II (which contained the privacy principles) and Annexes I and III to VII (which included the commitments and official declarations of the various US authorities). The level of protection of personal data guaranteed by the instrument was considered adequate by the European Commission in an adequacy decision, rendered pursuant to Article 25(1) of Directive 95/46 (Commission Implementing Decision (EU) No 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US privacy shield regime).

the new legal basis, capable of ensuring the transmission of personal information between the two sides of the Atlantic. The scheme was based on self-certification by American companies registered on a special list that their policies complied with the data protection and privacy standards set by the scheme[229].

On the one hand, the Privacy Shield constituted a significant evolution with respect to the Safe Harbour regime, with regard to the protection of privacy, being aimed to a greater extent at the empowerment of American companies and the strengthening of individual guarantees (both substantive and procedural). On the other hand, the system itself, by not expressly referring to the fundamental principle of legitimate purpose and providing for the possibility of derogation from the principles contained therein for reasons of public security, allowed the implementation of massive surveillance of personal data. These critical issues were also highlighted by the European institutions and bodies, which considered the system outlined in this way unable to adequately comply with European parameters on the protection of personal information and, ultimately, incompatible with the relevant EU legislation[230].

The Schrems II ruling is therefore set in this context of particular delicacy and complexity, characterised by: a) the obvious structural divergences between the US and the EU in relation to the safeguarding of individual privacy; b) the strong criticism that has accompanied the Privacy Shield regime since its adoption; c) the entry into force, in 2018, of the new European Data Protection Regulation, which has set strict data parameters for the protection of the legal situations at issue[231].

5.2.2. Schrems II

The Schrems II[232] decision stems from the request for a preliminary ruling by the Irish High Court in the context of seven years long-running dispute between the Austrian citizen, Mr. Schrems, and Facebook-Ireland, the subsidiary of Facebook Inc. It follows the decision of the Court of Justice, as noted above, to annul Decision No 2000/520 in the well-

[229] Annex II, par. I.2.
[230] Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, WP 238, 13 April 2016; European Parliament, Resolution on Transatlantic Data Flows, 26 May 2016; European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, 30 May 2016.
[231] Supra Michele Nino, '*La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*', at 738.
[232] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559

known Schrems I judgment of 2015 and the consequent declaration of invalidity of the Safe Harbour system invalid. In this second phase of the judgement, the referring court annulled the Irish Commissioner's rejection decision and asked the latter to re-examine the complaint lodged by Mr Schrems in 2013. The Irish authority launched an investigation and invited the Austrian citizen to reformulate such a complaint, also in light of the annulment of the EU-US data transfer regime ordered by Luxembourg. In that context, Facebook-Ireland acknowledged, both in the course of the investigation by the Irish authorities and in response to an express request by Mr Schrems, that the flow of personal information of users of the Facebook social network from the EU to the United States took place predominantly by virtue of the standard contractual clauses contained in Decision No 2010/87. In view of this, the Irish Commission, agreeing with the reasons expressed by the Austrian citizen in the complaint, contested the suitability of these clauses to constitute a valid basis for the transfer of data between the two sides of the Atlantic. processing only contractual rights to be enforced against the exporter and importer of the data, and not binding on the US authorities, were not capable of remedying the deficiencies inherent in the law in question. This was due to the fact that the US legal system, by conferring broad powers on US authorities - such as the FBI and the NSA - allowed the implementation of mass surveillance programmes of personal information, which were incompatible with Articles 7, 8 and 47 of the Nice Charter.

Therefore, the Commissioner, considering that Mr Schrems' reformulated complaint raised a question as to the validity of Decision No 2010/87, referred the matter to the Irish High Court, which, considering the arguments put forward by the Commissioner to be well-founded, referred eleven questions to the EU Court of Justice for a preliminary ruling, which may be summarised as follows: 1. Whether Regulation 2016/679 applies with regard to the transmission of personal data between economic operators, where such data may be processed in a third country for the purposes of public security and state security[233]; 2. What level of safeguards applies to standard contractual clauses adopted pursuant to Article 46 of the GDPR[234] ; whether national supervisory authorities are obliged to suspend or prohibit a transfer of personal information, carried out on the basis of those clauses, when they consider that those clauses are not capable of ensuring an adequate level of protection of that information, as provided for in Articles 45 and 46 of the GDPR and in the Nice Charter[235] 4. If Decision No 2010/87 is valid in the light of Articles 7, 8 and 47 of that Charter 5. Whether

[233] *Schrems II*, par. 80.
[234] *Ibid*, par. 90.
[235] *Ibid*, par. 106

the Privacy Shield ensures an adequate level of data protection, as required by Article 45 of the GDPR and the Charter itself[236].

5.2.3. Invalidity of the Privacy Shield, fundamental clarifications on DPAs and end of the saga

In the context of the numerous preliminary questions submitted to it, the Court deals with a profile of particular interest, concerning the exercise of the powers of the national data supervisory authorities under Article 58(2) of the GDPR, also in relation to the powers attributed both to the European Commission and to the national courts in this specific area. The judges of Luxembourg, through a very structured reasoning, come to define the powers at issue, with reference both to adequacy decisions and to standard contractual clauses, contemplated respectively by Articles 45 and 46 of the Regulation

With regard to the first instrument, the Luxembourg judges – confirming the principles set out in the Schrems I judgment – state that national supervisory authorities are bound to the adequacy decision of the European Commission, even when they consider that the third country concerned by that decision does not provide an adequate level of protection of personal information. Therefore, DPAs do not have the power to adopt acts contrary to it or to review its legitimacy, this being the sole and exclusive prerogative of the Court of Justice of the EU[237]. Moreover, this circumstance does not preclude these authorities - in the event that they are approached by those concerned by the processing of their data - either from analyzing the compliance of the cross-border transfer of such data with the relevant European legislation, or, if they have doubts as to such compliance, from referring the matter to the national courts, so that they may, if appropriate, raise a preliminary question on the validity of the transfer at issue before the Luxembourg courts.

On the other hand, with regard to the second instrument mentioned, much broader and more incisive powers are conferred on national supervisory authorities, establishing that, by virtue of Article 58(2), the latter are obliged to suspend or prohibit a transfer of personal information from the EU to a third State carried out on the basis of the standard contractual

[236] *Ibid*, Par 160
[237] Schrems II, cit., par. 116-118; see also Schrems I, cit., par. 61-62.

clauses, if they consider that such clauses are not complied with in that State and that European data protection law cannot otherwise be guaranteed[238].

The Court thus defines the competences of the authorities under discussion, as enshrined in the GDPR, contributing to greater clarity on the provisions contained therein and better specifying the relationships between the various institutions and bodies in charge of verifying the legitimacy of the transfer of personal information from the EU to third countries. More precisely, on the one hand, its previous case law is recalled and confirmed, according to which, with regard to data transfers based on adequacy decisions, the aforementioned authorities play a secondary role, compared to the primary role played by both the European Commission and the Court itself; On the other hand, important new principles are affirmed with regard to transfers of personal information based on standard contractual clauses, recognising the national supervisory authorities a remarkably active and autonomous part in this area, through the imposition of significant obligations on them and the attribution to them of significant responsibilities. The Court then goes on to analyse the most important issue, namely the validity of Decision No 2010/87 in light of Articles 7, 8 and 47 of the Nice Charter. It

It asks, namely, whether the standard contractual clauses provided for in Article 46 of the GDPR ensure an adequate level of data protection under the relevant EU legislation. The Court thus comes to accept the validity of the data protection clauses in Article 46 GDPR on the basis of the EU Charter, provided that these further offer additional guarantees and effective control mechanisms. In essence, it confirms the validity of the instrument in question, conditional on compliance with certain parameters, establishing the legitimacy of a decentralized system for checking the compatibility of the transfer of personal information from the EU to a third country with the relevant European legislation. More precisely, it is a decentralized system for verifying the adequacy of the level of protection offered by that country, based on the attribution of significant responsibilities, mainly to private bodies (data controllers or processors and recipients of the transfer), and, in a subsidiary way, to public bodies (national supervisory authorities and the European Data Protection Committee), ultimately excluding the European Commission from this verification.

Finally, the Court of Justice, although not directly addressed on this point, tackles the last (thorny) issue, concerning the validity of the "Privacy Shield" decision adopted by the

[238] Schrems II, par. 121 *see* also Christopher Kuner '*The Schrems II Judgment of the Court of Justice*', European Law Blog, (2020) available at https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

European Commission, asking itself, in particular, whether the US legal system is able to ensure an adequate level of data protection in accordance with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, and, therefore, equivalent to that offered by the EU legal system[239]. The European judges find that the provisions in question are contrary to the relevant European data protection legislation and do not comply with the principle of proportionality, as they are not limited to what is strictly necessary[240]. The Court, noting the inability of the US legal system to ensure a level of protection equivalent to that required by EU law, declares the Privacy Shield invalid with immediate effect, as it does not comply with the parameters contained in the relevant European legislation on data protection and, in particular, with Articles 7, 8 and 47 of the EU Charter[241]. Thus, the incorrectness of the adequacy assessment made by the European Commission is declared, with reference to the US legal system, and the illegitimacy ex nunc of the transfers of personal information from the EU to the United States, implemented on the basis of Decision No 2016/1250, is also established.

5.2.4. Implications of the case: a stronger GDPR

Bearing this in mind, it should be noted that the ruling is significant in that it confirms and enhances the consolidated (and appreciable) jurisprudential orientation developed by the Court over the last decade, aimed at granting enhanced protection to the rights to data protection and privacy and qualifying them as fundamental human rights[242]. As part of this approach, in the Schrems II case, the Court positioned itself as the guardian of the protection of the legal situations indicated, taking the Charter of Nice as an indispensable reference parameter for assessing the flow of personal information from the EU to a third State. It emphasized that the protection of personal data is not merely a domestic issue but a matter of global concern. As data continues to flow across borders, the EU seeks to ensure that its citizens' personal data enjoys strong protections no matter where it resides. This landmark decision has significantly impacted data protection regulations and international data

[239] *Ibid*, paras 150, 160-161; on this point, see: Case C-311/18, Opinion of Advocate General Henrik Saugmandsgaard Øe, ECLI:EU:C:2019:1145, paras 167-186.
[240] *Ibid*, paras 184-185.
[241] *Ibid*, par. 198-202
[242] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238; Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and al., ECLI:EU:C:2016:970.

transfers worldwide. Organizations involved in cross-border data flows must now navigate a more complex landscape, ensuring compliance with the GDPR's stringent requirements and assessing the adequacy of data protection measures in recipient countries. It has also prompted discussions around the need for stronger data protection standards and global cooperation to address the challenges of data transfers in the digital age.

Another significant profile to highlight in our analysis is the fact that this judgment reinforced the territorial scope of the European Data Protection Regulation both within and outside the EU legal system. The Court's approach is to be welcomed, since, on the one hand, it has clarified the scope of application of this regulation and has further defined the powers that can be exercised by national supervisory authorities[243] ; on the other hand, it established the applicability of a single legal standard - that of the equivalence of the level of data protection offered by the legal system of a third country - for assessing the legitimacy of transfers of personal information, carried out on the basis of both the adequacy decision and the contractual clauses (and implicitly also those implemented by virtue of binding corporate rules)[244]. In this way, not only consistency in the regime established by Regulation No 2016/679 and unity in its application were ensured, but also greater legal certainty with regard to the subjective legal situations safeguarded by Articles 7, 8 and 47 of the EU Charter[245].

In addition, while declaring the validity of the standard contractual clauses, the Court nevertheless questioned their functioning and execution[246] and proposed a new formulation, which is more oriented towards the protection of human rights. This prevents the clauses from being used by commercial companies as mere legal fictions: In fact, in the past, in order to legitimise the transfer of data from the EU to third States, these companies have limited themselves to inserting them in their contracts, thus respecting the formal aspect (i.e. ensuring that the transfer was accompanied by contractual guarantees), but disregarding the substantial fact, i.e. the concrete implementation of the mechanism in question and the concrete risk that the intelligence authorities of the third country could easily have access to such data and use them for law enforcement purposes under the relevant national legislation.

[243] Supra Christopher Kuner, '*The Schrems II Judgment of the Court of Justice*'.
[244] European Data Protection Board, Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020, available at edpb.europa.eu, p. 3, para. 6.
[245] Theodore Christiakis, 'After Schrems II', European Law Blog, (2020) available at https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.
[246] Data Protection Commission, "DPC Statement on CJEU Decision", (2020).

Ultimately, the Court, through its chosen approach, implicitly subjects to criticism the standard contractual clauses in the way they have been implemented so far to make the extra-EU flow of personal information possible[247]. The ruling under review calls, firstly, for an improvement in their functioning (which is since than been happening)[248], in order to make them an instrument that is widely used in commercial and financial contexts, and at the same time is able to reconcile the requirements of safeguarding the rights to data protection and privacy with those of protecting national security. Secondly, it (the ruling) ends up raising the level of the protection threshold for information transferred from the EU to third States on the basis of standard contractual clauses - and also, indirectly, of binding corporate rules - by identifying certain and strict parameters, which state authorities and commercial companies must adhere to when processing such information.

6. GDPR's enforcement, how it started and how it is going

In the wake of its rollout, the GDPR faced both anticipation and skepticism. While celebrated as a substantial advancement in safeguarding individuals' privacy rights, it also encountered criticism for its complex requirements and challenges in enforcement[249] gathering questions on whether the regulation could fully live up to its ambitious goals or merely remain an aspirational vision. Critics were justified, as the GDPR was designed as the globe's toughest privacy law, emphasizing large fines— EU's DPAs can impose sanctions up to €20 million (roughly $20,372,000) or 4% of a firm's global revenue in case of non-compliance – in order to provide an impetus to implement these policies sooner rather than later. Policymakers basically trade off the size of fines with the probability of

[247] *Supra* Michele Nino, '*La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo'*,, at 753.
[248] See Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance); ELI: http://data.europa.eu/eli/dec_impl/2021/914/oj
[249] *See inter alia* Anda Bologa, *'Fifty Shades of GDPR Privacy: The Good, the Bad, and the Enforcement'*, CEPA, (2023); Matt Burgess, '*How GDPR is failing',* Wired, (2022) available at https://www.wired.co.uk/article/gdpr-2022; Marco Massimini, *'Effetto GDPR depotenziato tra debolezze di enforcement e "braccino" irlandese'*, Privacy.it, (2021) available at https://www.privacy.it/2021/10/04/gdpr-depotenziato-debolezze-enforcement-massimini/; Supra Giulia Gentile and Orla Lynskey, '*Deficient by design? The transnational enforcement of the GDPR. International and Comparative Law Quarterly'*, at 800.

levying a fine to ensure compliance[250], choosing a severe penalty structure which may (and did) have an impact on how much effort is put forth to comply with the GDPR by both domestic EU businesses and foreign businesses that market to EU consumers. It would not have been long that, in response, some services completely shut down, while others restricted access to users in the EU. For instance, several multiplayer games in the EU were discontinued due to the need for infrastructure changes, including Uber Entertainment's Super Monday Night Combat and Gravity Interactive's Ragnarok Online[251], whereas the changes around user consent for data processing resulted in the shutdown of advertising companies like Drawbridge[252]

Nevertheless, did have a rough start, with only a few fines issued by EU regulators during the 2018 time frame. 2019 fell short as well with only 91 reported fines (and charges as high as 50 million euros[253]) leading the same European Commission[254] to acknowledge the problem. The enforcement of the GDPR faces additional challenges due to the decentralized nature of its enforcement framework, which relies on the collaboration and coordination of national Data Protection Authorities (DPAs). Each EU member state is responsible for its own DPA, which means that enforcement actions can vary across jurisdictions, leading to potential disparities in the level of enforcement. The existence of multiple DPAs means that enforcement efforts may be influenced by the specific legal and cultural contexts of each member state. Variations in resources, priorities, and approaches to enforcement of course have an impact on the uniformity of GDPR enforcement across the EU, but at the same time they can be seen as an opportunity.

Despite these challenges, it is essential to recognize that the decentralized enforcement system also brings benefits, as it allows DPAs to have a better understanding of local circumstances and the specific challenges faced by their constituents. It fosters a nuanced approach to enforcement that can be tailored to address regional concerns effectively. As time passes, there is an ongoing effort to strengthen the cooperation and coordination among national DPAs to ensure a more harmonized and consistent enforcement

[250] Johnson, Shriver, and Goldberg '*Privacy & Concentration: Consequences of GDPR Management Science'*, Articles in Advance, pp. 1–27, (2023) at 2 citing the study of Mitchell Polinsky, Steven Shavell, '*The economic theory of public enforcement of law'*(2000). Journal of Economic Vol. 38 No.1, Literature 45–76.
[251] Owen S. Good, '*Super Monday Night Combat will close down, citing EU's new digital privacy law'*, Polygon, (2018) available at https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr
[252] James Hercher, '*Drawbridge Exits Media Business In Europe Before GDPR Storms The Castle'*, AD exchanger (2018) available at https://www.adexchanger.com/mobile/drawbridge-exits-media-business-europe-gdpr-storms-castle/
[253] Gdpr fines. https://www.dlapiper.com/en/uk/insights/ publications/2019/01/gdpr-data-breach-survey/
[254] Commission Nationale de l'Informatique et des Libertes Online, *'Targeted advertisement: What action plan for the CNIL?'* Report, Commission Nationale de l'Informatique et des Libertes (2019).

approach which culminated in April with the Commission' Contribution[255], which seeks to give guidance in order to improve both the cross border and internal flow of data[256]. The European Data Protection Board (EDPB) plays a vital role in facilitating this collaboration, offering guidelines and promoting best practices to support a more coherent enforcement landscape.

While researchers suggest that time will be needed for a fully satisfactory result[257]. the trend appears to be indeed slowly getting better: taking the numbers of fines as parameter, we can see as they are constantly growing with 462 fines recorded in 2021 and 532 in 2022. 2023 witnessed the biggest fine ever recorded, with 1.2Billion Euros fine issued to Meta by the Irish Data Protection Commission[258] in conclusion to the Schrems Saga. Surprisingly, this single fine alone is very nearly equal to or exceeds the total amount of GDPR fines assessed by January 28, 2022 (€1.64 billion). The total amount of GDPR fines has now surpassed €4 billion: these numbers show the ongoing dedication to upholding data protection laws and draw attention to the growing financial costs of non-compliance.

6.1 EU's SA aligned: Cleaview AI sanctions

The sanction issued against American company Cleaview AI provides a good example of how important and disshuasive concerted action in enforcing GDPR can get when duly operated. On the 23rd of May Austrian SA joined an increasingly long list of regulators – namely France, UK, Italy and Greece in the EU along with Canada and Australia – issuing an order[259] against Clearview AI.

Using its unique facial recognition algorithm, Clearview AI "scrapes" images of people's faces from publicly accessible sources and extracts biometric data from each image. In this way, the company claims to have gathered over 20 billion facial images. Most often law enforcement agencies, Clearview AI's clients can upload a photo of a person's face,

[255] Contribution in the context of the Commission initiative to further specify procedural rules relating to the enforcement of the General Data Protection Regulation, European Data Protection Supervisor, (2023).
[256] *Ibid,* "The EDPS wishes to stress that the need for effective and efficient cooperation is not limited to cross-border cases involving multiple national DPAs. The same need exists in cases where personal data flows from Union institutions, bodies, offices and agencies (EUIs) to public bodies or private entities within the European Economic Area (EEA), and vice-versa"
[257] See Oxford Analytica, *'GDPR enforcement will improve slowly in the EU'*, Expert Briefings, (2022).
[258] Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation.
[259] Decision by the Austrian SA against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR, https://edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en

which can then be compared with an entry in its database. The business then offers a link to the image's original source, which should reveal who the subject of the client's uploaded photo is. On its site, the company states “Clearview AI’s revolutionary investigative platform enables quicker identifications and apprehensions to help solve and prevent crimes, helping to make our communities safer”. However, Clearview AI's business strategy is very contentious, and the company is facing numerous legal challenges from opponents who want to put an end to it.

The sanctions against Clearview AI across various European jurisdictions underline a concerted alignment of the European Supervisory Authorities (SAs) and rapresent a unique case of unified stance on adherence to the General Data Protection Regulation (GDPR). The following dissection of individual cases across Italy, France, Greece, and Austria highlights this trend:

Everything started when France when the CNIL (French Data Protection Authority) began its investigation into Clearview AI's facial recognition platform. In May 2020, the authority received complaints from individuals about difficulties in exercising their rights of access or erasure. People who used the facial recognition platform from Clearview AI complained to the CNIL in May 2020 about the challenges they faced when attempting to exercise their right of access or right to be forgotten. The group Privacy International also alerted the CNIL to this practice the following year, which ultimately resulted in the opening of an investigation. Since the data was gathered and used without a proper legal basis and in violation of people's rights, particularly their right to access, the investigation by CNIL revealed violations of Articles 6, 12, 15, 17, and 31 of the General Data Protection Regulation (GDPR) regarding the unlawful processing of personal data.

The CNIL gave CLEARVIEW AI formal notice[260] on November 26, 2021, giving it two months to stop collecting and using data about people on French soil without a justification, to make it easier for people to exercise their rights, and to abide by erasure requests. However, Clearview AI didn't respond in any way.

The investigation found that Clearview AI's facial recognition software uses a collection of face-containing images for commercial purposes, such as providing information to US law enforcement agencies, without the consent of the individuals whose personal data had been processed or a legitimate interest in collecting and using that data.

[260] Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI, https://www.cnil.fr/sites/cnil/files/atoms/files/decision_ndeg_med_2021-134.pdf

The intrusive and overwhelming nature of the process, which gathers images of millions of people in France who do not reasonably expect their images to be processed by the company to supply a facial recognition system used by States for law enforcement purposes, was specifically addressed by CNIL.

According to the complaints made to CNIL in 2020, the investigation found that Clearview AI does not make it easier for data subjects to exercise their right of access. In addition to limiting the use of this right to data collected only within the previous twelve months prior to the request, Clearview AI also limits its use to twice annually and only responds to some requests after receiving an excessive number of them from the same person. Additionally, the company only responded partially to the right to be forgotten and did so ineffectively.

Taking into consideration serious risks to the fundamental rights of individuals, the massive nature of the processing, and the lack of cooperation with the data protection authority, CNIL fined[261] Clearview AI issuing a maximal fine of €20 million and a penalty of €100,000 per day of delay following two months after the decision. CNIL also issued an order to Clearview AI to stop the processing and collection of personal data of individuals in French territory and to delete personal data that has been collected without a proper legal basis

Italy soon followed suit, imposing a massive €20 million penalty[262] on Clearview AI for collecting and processing biometric data illegally through facial recognition techniques. This decision was aligned with France's concerns, particularly focusing on violations of GDPR Articles 5, 6, 9, 12, 14, 15, and 27. Italy's privacy authority also ordered Clearview AI to appoint a representative within the EU to facilitate the exercise of citizens' rights.

The Hellenic Data Protection Authority (HDPA) in Greece further intensified the scrutiny on Clearview AI. In a decision dated July 13, 2022, the HDPA imposed a fine of €20 million[263], aligning with the Italian and French authorities in recognizing the violation of key GDPR principles. Like the Italian authority, Greece also ordered the cessation of biometric data processing and the deletion of already accumulated personal data.

---

[261] Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI, https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf

[262] Ordinanza di ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362] , https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751362

[263] ΑΠΟΦΑΣΗ 35/2022 , https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym.pdf

Finally, the Austrian supervisory authority (DSB) took a comprehensive view of the issue and expanded on the findings of its European counterparts. On May 10, 2023, the DSB issued a decision against Clearview AI, detailing specific infringements related to GDPR Articles 5, 6, 9, and 27. This investigation underscored the unlawful and unfair processing of personal data, and the Austrian SA ordered Clearview AI to erase the complainant's personal data and to designate a representative within the EU. The company was even the object of a resolution[264] adept by the EU Parliament in order to ban the use of private banks for face recognition.

These consistent fines, along with Austria's orders to erase data, underline a collective European stance that emphasizes the protection of individual rights in the age of advanced biometric technology. Further alignment can be seen in the demands for Clearview AI to designate a representative within the EU, a move aimed at ensuring easier access to legal rights for citizens. Moreover, the French case's unique focus on the company's non-cooperation with the data protection authority adds an additional dimension, underscoring the need for cooperation between technology firms and regulatory bodies. Beyond the uniformity in the imposition of fines and data erasure, the complexity of these legal actions lies in the deliberate balance struck between collective enforcement and individual state autonomy, considering the legal and cultural variances in each jurisdiction.

The synchronized approach against Clearview AI sets an unambiguous precedent, one that will hopefully shape future legal actions against tech firms engaged in unauthorized data collection and processing within the EU. The robust and decisive nature of these decisions, taken within the framework of a shared European jurisprudence, signals a critical shift in regulatory control, reinforcing the notion that compliance with the GDPR is non-negotiable, and that violations will be met with significant penalties.

7. GDPR striking the balance

In this chapter, in examining both the theoretical framework and practical enforcement of the GDPR, we have delved into the Regulation's main provisions, analyzing

[264] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

its strengths and weaknesses by building on the premise that it is only through a holistic perspective that the discipline it sets forth can be better appreciated.

While focusing solely on one aspect may lead to dissatisfaction, we have shown how the Regulation provides clear principles, rules, and mechanisms that seek to foster a thriving internal market without sacrificing the essential protections for individual privacy in an age where personal data is a highly prized asset.

Stemming from an internal-market-driven perspective, we have outlined the origin and development of what we named the "fifth freedom" for the movement of data, and how crucial this is in our data-driven society in order for the EU to remain competitive globally.

Afterwards, we tackled the extent and limits of the privacy framework laid down by the Regulation and analyzed whether this may results hindered by the Regulation's provisions on fostering the market. The analysis showed quite the opposite result since privacy concerns never appear to be put in discussions and prevail in the decisions of the Court.

Clearly, for achieving its best practice deeply requires the coordinated efforts of the European Union (CJEU) and Supervisory Authorities (SAs) or Data Protection Authorities (DPAs). These institutions play integral roles in interpreting, enforcing, and adapting the GDPR to the complex realities of the modern digital environment.

In sum, the GDPR drafting reflects an awareness of the technological landscape and the legal challenges specific to data protection, an always evolving and ever-changing landscape which can not be addressed with the specificity some desire (hence the critics towards its alleged vagueness, we built up on this in the ADM analysis) as it would turn out to be inadequate and outdated in the right moment it is issued[265]. By taking this into consideration, it presents a framework that attempts to balance the rights of individuals with the requirements of the digital internal market, and notwithstanding the difficulty of the task, being them quasi-opposite interests, the Regulation does a commendable job. It provides a legal structure that businesses can follow while safeguarding individual rights, demonstrating that one can actually foster the other. Data Subjects, of course, remain the ones who benefit the most from this framework as the highly demanding compliance

[265] On the topic of the GDPR being deliberately vague, see Luke Irwin, '*GDPR: Understanding the 6 data protection principles'*, in IT Governance European Blog, (2021); Thomson Reuters, '*Top Five Concerns with GDPR Compliance'*, (2017); Aashaka Shah, Vinay Banakar, Supreeth Shastri, Melissa Wasserman, and Vijay Chidambaram, *'Analyzing the Impact of GDPR on Storage Systems', 11th U*senix Workshop, at 2; 'Making Sense of the General Data Protection Regulation (GDPR)', Tripwire Blog, (2017) and Wolfgang Hauptfleisch, '*GDPR — Establishing A Fundamental Right, Not Just Regulation'* Medium, (2022).

requirements set out for organizations in the EU shields them from intrusive and/or harmful processing.

In this respect, the GDPR appears to be more appreciated beyond the EU borders, where the Regulation enjoys such an excellent reputation that it is considered a golden standard of data protection. This will be the focus of the next and last Chapter, in which we conclude our overall analysis of the Regulation in light of the current global trends and contrasting perspectives on data protection.

CHAPTER III - HOW GDPR SETS THE GLOBAL STANDARD IN DATA PROTECTION

1. The GDPR in Europe and beyond

In the previous Chapters, we analyzed GDPR as a multifaceted Regulation which has had profound implications for EU based administrations, companies and users. Stemming from the Regulation's provisions and the decisions from the Court of Justice we also tackled how GDPR's reach extends far from the EU borders. Indeed, we have seen how in *Google-Spain* the Court of Justice applied EU data protection legislation to a foreign service provider, determining that the DPD applied to Google, a US company, also because Google's establishment in an EU Member State[266], given that it covers the personal data of all EU residents, regardless of the location of the processing.

Nevertheless, as this Chapter will show, the impact of the GDPR abroad goes much further, with the wide territorial scope being one of the two elements – the other being the expanded definition of personal data – whose combination have been identified[267] from scholars to ensure a global impact from the GDPR. As to the former element, scholars[268] analyzed the "extraterritorial" application of EU law on data protection identifying its juridical bases under international law. First, it could be argued that the extraterritorial reach of EU data protection law is strongly based on territoriality given that it is triggered by a person or activity having a territorial connection to the EU[269]. According to the GDPR, territoriality may even be the fundamental tenet, with the application of the Regulation to organizations based outside the Union being triggered by their targeting or monitoring of individuals in the Union. This process has also been helpfully referred to as "territorial extension[270]" in the literature. Second, individual rights based on a person's demonstrable

[266] Supra CaseC-131/12,Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, paras. 55–56.
[267] *See* Michelle Goddard, '*The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*', International Journal of Market Research Vol. 59 Issue 6, (2020), at 703.
[268] Cedric Ryngaert, Mistale Taylor, '*The GDPR as global Data Protection Regulation?',* Symposium on the GDPR and International Law Vol.114, Cambridge University Press, (2020), at 6.
[269] *Ibid.*
[270] *See* Joanne Scott, '*Extraterritoriality and Territorial Extension in EU Law'*, 62 American Journal of Comparative Law, Vol. 62, No. 1, (2014).

affiliation to the EU—typically, citizenship or residence—are related to the broad geographic reach of EU data protection legislation. Therefore, the EU's claims are supported by the passive personality principle, which enables the EU to defend its citizens or residents, such as when data transfers involving EU subjects are made to less than ideal jurisdictions[271]. As to the definition of personal data, we have already tackled how far-reaching this concept emerges from Luxembourg's extensive case law (Nowak, Breyer, the same Google Spain), emerging as a much wider concept of personally identifiable information (PII) under US privacy law[272].

Notwithstanding the main causes behind this result, nowadays there is an almost unanimous consensus around the fact that GDPR has become a *de facto* standard worldwide[273] The aim of this concluding chapter is to elucidate how this regulatory standard and jurisdictional model was set and appreciated globally while also exploring the measures that can be undertaken to sustain it. While initial responses outside EU borders were characterized by apprehension and skepticism[274] towards the Regulation, we will track the journey that prompted even its fiercest critics between stakeholders and researchers to advocate for data protection frameworks inspired by the GDPR, and the adoptions of such norms all over the world.

In order to proceed, we shall commence by evaluating the outcomes of the Regulation as we approach its fifth year being effective, with the objective of discerning what can have rendered the General Data Protection Regulation (GDPR) so well-regarded within the international arena. We will focus on the initial challenges faced by businesses in adapting to the GDPR framework: this will involve shedding light on the operational hurdles, compliance difficulties and the potential for increased costs. Moving forward, we will delve into the transformation of this narrative, emphasizing how many of these challenges transformed into opportunities. By embedding the principles of the GDPR into their operational frameworks, businesses not only enhanced their data protection mechanisms but also appear to have gained a competitive advantage. Improved consumer trust, enhanced

---

[271], See Cedric Ryngaert, Mistale Taylor, '*The GDPR as global Data Protection Regulation?'*.

[272] *See* Michelle Goddard, '*The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*', at 703.

[273] Rosylin Layton and Silvia Elaluf-Calderwood, '*A Social Economic Analysis of the Impact of GDPR on Security and Privacy* Practices', 12th CMI Conference on Cybersecurity and Privacy (CMI), (2019) at 1; Corinne Bernstein, '*Personally Identifiable Information (PII)*', TechTarget, (2023); Josep Domingo-Ferrer, '*Personal Big Data, GDPR and Anonymization'*, Flexible Query Answering Systems, Vol 11529 (2019), at 7.

[274] Inter alia, see Roslyn Layton, Julian Mclendon, '*The GDPR: What It Really Does and How the U.S. Can Chart a Better Course'*, The Federalist Society Review Volume 19 (2018); Ivana Kottasová, '*These companies are getting killed by GDPR'*, CNN Business, (2018); Jedidiah Yueh, '*GDPR will make BigTech even bigger*', Forbes Technology Council, (2018);

brand reputation, and a streamlined data management system are among the several different benefits companies reaped, turning initial skeptics into advocates of the Regulation.

Having established the business paradigm shift, the chapter will then shift its attention to the global impact of the GDPR's success. Recognizing the need for a comprehensive data protection framework, numerous countries began to emulate the GDPR, drafting regulations influenced by its principles. We will explore specific examples of nations that have incorporated GDPR-like standards, underscoring the Regulation's evolution from a European mandate to a global gold standard in data protection.

Finally, we will tackle the Regulation's relation with emerging technologies, the frictions that emerged during these years and how they can be overcome in order for the EU to maintain its position as leader in the realm of data protection law in the global digital economy[275].

2. GDPR as global standard: "Brussels Effect" or deliberate choice based on results?

The perception of the GDPR, when it was first introduced, of an arduous mandate that businesses would find burdensome to navigate and comply with was shared globally. However, our analysis will proceed to showcase how, as time progressed, more and more countries adopted data protection regulations which (in some cases explicitly) took the GDPR as reference.

The reasons behind this global movement towards GDPR-like laws was also identified from scholars[276] in the so-called "Brussels' effect[277]". The Brussels Effect refers to the EU's unilateral ability to govern global markets, without the need for international organizations or the participation of other States. Following this theory, the EU would have the capacity to enact legislation that shapes the worldwide business climate, resulting in a

[275] Craig McAllister, "*What about Small Businesses: The GDPR and Its Consequences for Small, U.S.-Based Companies,*" Brooklyn Journal of Corporate, Financial & Commercial Law 12, no. 1 (2017), at 212

[276] See Paul M. Schwartz, '*Global Data Privacy: The EU Way'*, New York University Law Review 94, no. 4 (2019), at 779; *Supra* Cedric Ryngaert, Mistale Taylor, '*The GDPR as global Data Protection Regulation?',* at 9; Simon Gunst, Ferdi De Ville, *'The Brussels Effect: How the GDPR Conquered Silicon Valley'*, (2021), 26, European Foreign Affairs Review, Issue 3, 437-458; Marco Luisi, '*GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion',* E-International Relations, (2022).

[277] Anu Bradford, '*The Brussels Effect: How the European Union Rules the World'*, Oxford University Press, (2020).

remarkable "Europeanization" of many crucial facets of global commerce[278]. Therefore, unlike many other forms of global influence, the EU does not need to impose its standards coercively on anyone as market forces alone are frequently sufficient to convert the EU standard into the global standard as corporations willingly extend the EU regulation to regulate their global operations[279].

While the theory has gathered much consensus, we also argue that tangible advantages emerging from within the EU's business landscape are not something to overlook. In this sense, adopting GDPR-like laws would reveal itself as a deliberate choice to mimic the balance the Regulation strikes and its consequent benefits on the market without sacrificing the rights of users. Following this argument, we will delve into the impact of GDPR in its geographical area of application to understand whether it achieved results which could be desirable for foreign countries to replicate.

2.1 Main results after 5 years of application

The General Data Protection Regulation of the European Union entered into force on 24 May 2016 and applies since 25 May 2018[280]. At the time, a lot was written about the initial compliance costs[281], the effects on businesses of all sizes[282], and whether it represented a change in the accepted standards for data privacy and security[283].

In light of what we have said in our previous chapters, what clearly emerges as the GDPR's main advantage is that it overcame the EU Member States inconsistent implementation by establishing a robust and consistent data breach law, in order to create a uniform standard. Notwithstanding the difficulties of the national-level implementation from data agencies and some still-standing different interpretations, GDPR has been recognized as achieving a satisfactory level of standardization and uniformity as emerges from the increase of data breach notifications[284].

[278] *Ibid*, at 15 (Introduction).
[279] *Ibid*.
[280] GDPR, Art. 99.
[281] Arun Subramanian, '*GDPR Cost and Implementation Concerns for Businesses'*, Medium, (2019); Alan McQuinn, Daniel Castro, '*The Costs of an Unnecessarily Stringent Federal Data Privacy Law'*, Information Technology and Innovation Foundation, (2019), at 2.
[282] Dror Liwer, '*GDPR: one size does not fit all'*, CSO online, (2018).
[283] Mark Scott, Laurens Cerulus, '*Europe's new data protection rules export privacy standards worldwide'*, Politico, (2018).
[284] See Jennifer Huddleston, '*Takeaways from the GDPR, 5 Years Later'* Commentary, CATO Institute, (2023).

Moreover, these first five years of application have helped in dispelling many of the myths surrounding the Regulation[285], especially those arguing of activities that would have been impossible on account of the fact that GDPR would not allow them. In summarizing them, one pervasive belief is that the GDPR invariably mandates consent[286] for the collection and processing of personal data. However, as we have seen, the Regulation outlines six lawful bases upon which personal data can be processed, directing entities to select the one most suited to their activities. At best, the problem could be the opposite, namely the fact that these bases can provide too much space of operation. Scholars also argued that GDPR's primary focus is imposing hefty fines on non-compliant entities[287]. While fines are indeed a part of the enforcement mechanism, they are reserved for the most egregious of violations. Numerous other remedies and corrective measures exist within the GDPR's enforcement toolkit such as reprimands, warnings, data processing bans, data rectification or erasure and counting. Finally, it is important to stress how GDPR does not hinder, let alone prohibit data sharing[288]. In actuality, the Regulation encourages transparent, lawful, secure, fair, and proportionate data sharing.

Furthermore, the last five years have demonstrated that GDPR compliance is not the insurmountable hurdle initially presented[289]. The effective implementation of GDPR by businesses underscores the significance and impact of the Regulation, especially given the initial reservations and discussions around it. In the following section, we will further examine this transition and its broader consequences on the internal market.

2.2 GDPR and business results

When full General Data Protection Regulation (GDPR) compliance was finally achieved by the May 25, 2018 enforcement deadline, every impacted business leader in the world was allegedly thrilled[290]. After a period of five years, it's essential to assess the response of businesses globally to the GDPR as well as its influence on other countries. We

[285] See Philippa Donn, *'GDPR 5 years on'*, Data Protection Network, 2023 and '*Data Proetction Officers: Myth Buster'*, Data Protection Network, 2022 and European Commission's Guidelines on Data Protection Officers ("DPOs")
[286] Neil Richards and Woodrow Hartzog, *'The Pathologies of Digital Consent'* , Washington University Law Review, (2019) 1461.
[287] For an in-depth focus, *see* Andrew Clearwater, Brian Philbook, '*GDPR Enforcement: Is it really about the fines*?', The International Association of Privacy Professionals, (2019).
[288] See Antonia Vlahou et al. '*Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics?'.* Hypertension vol. 77, No.4, (2021), at 1029.
[289] Luke Irwin, '*Organisations struggling to meet GDPR requirements, with poor planning and lack of awareness to blame*', IT Governance Blog, (2019); Tal Z. Zarsky, '*Incompatible: The GDPR in the Age of Big Data*' Seton Hall Law Review, (2017) at 995.
[290] Anthony Jones, *'GDPR Three Years Later, What Impact Has it Made*?' for Partners, (2022).

will begin our examination by tackling the initial difficulties, pointed out by both scholars and stakeholders, in order to understand whether those concerns actually stood out to the test of time.

2.2.1. Initial difficulties

A new Regulation brings with it benefits and costs, being able to stimulate ideas as well as hinder their implementation[291]. The introduction of the GDPR admittedly marked a momentous shift in data protection law (with authors even referring to "tidal waves"[292]), prompting businesses to deeply reconsider and restructure their data handling and processing mechanisms. The profundity of the change, while geared towards safeguarding individual rights, was not without its set of concerns for the entities expected to comply. Both scholars and undertakings' first reaction, in fact, was one of discouragement and fear of a Regulation that for some seemed even impossible to be compliant with[293] and this for several reasons.

While the emerging concerns varied (the Regulation was initially referred to as too complex[294], as involving too much subjectivity, as costly in requiring for companies extra administration staff and expert DPO[295] staff, extra employee training with the consequent difficulties in recruiting and *altera[296])*, they can all be summarized in calling out the time and expense of the implementation of the new provisions, basically inconsistent with the way to conduct business[297]. Among scholars, on the other hand, the common idea was that these stringent regulatory restrictions were likely to impact undertakings' performance and persuade some to cut their service offering in the EU in order to avoid cost and risks that outweigh the benefits[298]. It is worth noting that while this phenomenon admittedly took place during the first years of implementation, its scale was much inferior to the expectations, accounting mostly of small companies from the US[299].

---

[291] Gerard Buckley, Tristan Caulfield, Ingolf Becker '*It may be a pain in the backside but...*" *Insights into the resilience of business after GDPR'*, Proceedings of the 2022 New Security Paradigms Workshop, (2022) at 21.
[292] Samuel Greengard, *'Weighing the impact of GDPR'*, ACM Volume 61, Number 11 (2018), at 16.
[293] *Ibid,* citing Attorney Tanya Forsheit who stated *"It is simply not possible to be 100% compliant*".
[294] Sean Sirur, Jason R.C. Nurse, Helena Webb, '*Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*' ArXiv, (2018), at 3.
[295] GDPR, Art. 37 establishes the cases in which a controller and a processor must designate a data protection officer (DPO).
[296] *Supra* Gerard Buckley, Tristan Caulfield, Ingolf Becker '*It may be a pain in the backside but...*" *Insights into the resilience of business after GDPR'*.
[297] For an in-depth analysis of the most common concerns, see Adam Faifr, Martin Januska, '*Companies' readiness of GDPR and implementation barriers*', 41st International Academic Conference, Venice, (2018).
[298] See Stephane Ciriani. '*The Economic Impact of the European Reform of Data Protection'* Communication & Strategies, Vol *No.97*, (2015), at 52.
[299] In specific, *see* Hannah Kuchler, '*US small businesses drop EU customers over new data rule'*, Finanacial Times.

As mentioned, an immediate challenge encountered for companies was the scarcity of seasoned privacy professionals, with Article 37 (5) of GDPR explicitly requiring for the data protection officer to be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39[300]. As businesses grappled with understanding and complying with the complex provisions of the Regulation, the demand for experts in the field surged significantly. Finding these experts, with the nuanced understanding and experience required to guide businesses, became a daunting task[301].

Further complicating matters, there was pervasive uncertainty surrounding the practical aspects of GDPR compliance[302]. A considerable number of companies were uncertain about the intricacies of implementing and managing data as per GDPR mandates. This uncertainty was exacerbated by a lack of clarity about the expertise or staff needed to undertake essential activities like data protection impact assessments (DPIAs)[303].

These complexities largely emanated from the radical shift that the GDPR presented. The novelty of the Regulation and the comprehensive framework it established marked a departure from the relatively lenient pre-GDPR era. Undertakings, having been accustomed to a more liberal data handling environment, found themselves navigating the stringent labyrinth of GDPR stipulations, striving to balance compliance with operational efficiency. Nevertheless, it would not have been long until both businesses and scholars would have acknowledged that what was born as compliance nightmares would have swiftly turned out into opportunities[304].

---

[300] GDPR, Art. 39(1), namely: to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; to cooperate with the supervisory authority; to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

[301] Joe Garber, Micro Focus, '*GDPR – compliance nightmare or business opportunity*?', in Computer Fraud & Security, (2018), at 15.

[302] WatchGuard Technologies, Survey Showing Confusion Around GDPR Compliance, available at https://securitybuyer.com/survey-shows-global-organisations-unsure-gdpr/ .

[303] *Supra* Samuel Greengard, '*Weighing the impact of GDPR'*.

[304] *Supra* Joe Gaber*, 'GDPR – compliance nightmare or business opportunity?.* The author, in 2018 already, goes as far as stating: "Yet organizations stepping back to look beyond the fines should see the GDPR for what it really is – a big business opportunity".

2.2.2. Businesses after implementation: results

The five-year span from its adoption offers a good perspective to understand the Regulation's real-world effects beyond the initial and ongoing discussions. Despite the initial concerns, over the past five years worldwide undertakings have examined more closely how they handle the security and privacy of customer data, with the most immediate results constituting significant advancements in consumer data governance, monitoring, awareness, and strategic decision-making[305].

Research conducted from different scholars show in numbers how positive the impact of the Regulation has actually been since the very beginning: 89 percent of EU respondents to a survey[306] carried out just one year after the GDPR went into effect said they had hired a DPO in response to the Regulation (averting the worries about an alleged impossibility in the research) and awareness of the issues surrounding data protection had skyrocketed. The top three items on boardroom's agendas concerned compliance (83%), data breaches (68%) and privacy initiatives (61%). Moreover, it is worth emphasizing that Article 37 of the GDPR does not always mandate the designation of DPOs (such designation is only required in specific cases, as outlined above) and provides organizations with some flexibility in how they appoint DPOs Under the provisions of the GDPR, a single DPO may be designated for a group of undertakings[307] and in cases where the controller or processor is a public authority or body with a single DPO designate-able for several such authorities or bodies[308]. This takes into account their organizational structure and size.

Spending on training revealed itself as a hefty cost, as investments in training were cited as the top GDPR compliance priority for the upcoming year by nearly eight out of ten respondents. Other substantial costs were destined for the upgrade of the companies' IT infrastructure to make it GDPR compliant. Both of these, however, would have been soon recognized as beneficial. New data systems delivered new efficiencies and cost-savings[309], not to mention that study demonstrate that two out of six companies only had to make minimal changes to their infrastructure in order to make it compliant[310].

Essentially, rather than being a hindrance, GDPR compliance emerged as an incentive for efficiency-driven investments (at best, given that as seen many SMEs did not

[305] Supra Anthony Jones, *'GDPR Three Years Later, What Impact Has it Made*?'.
[306] Paul Breitbarth, ,'*The impact of GDPR one year on'*, Volume 2019, Issue 7, (2019), 11-13.
[307] GDPR, Art. 37(2).
[308] GDPR, Art. 37(3).
[309] Gerard Buckley, Tristan Caulfield, Ingolf Becker '*Insights into the resilience of business after GDPR'*, NSPW '22: Proceedings of the 2022 New Security Paradigms Workshop, (2022), at 27.
[310] *Ibid*.

require any) with tangible improvements that go beyond costs-saving[311]. In this sense, above mentioned DPIAs provides a perfect example. Article 35[312] of GDPR introduces the concept of Data Protection Impact Assessments, a systematic method for organizations to assess and manage data processing activities. If a specific type of data processing, especially when incorporating new technologies, is expected to pose a substantial risk to the rights and freedoms of individuals, the data controller is mandated under the provision to conduct an evaluation of how the planned processing activities will impact the safeguarding of personal data before proceeding with the processing.

Originally perceived as a compliance necessity, Ian Williams Head of Data Protection at Railpen and experienced DPO listed[313] many of the benefits DPIAs bring along: among others, they save money, time and effort; reduce risks by steering companies away from developing products and services that incur regulatory intervention or sanction (and consumer backlash damaging brands and potentially resulting in compensation claims) and go to increase the trust from data subjects whose personal information is handled by your organisation by identifying good controls to keep it safe and avoid mishandling incidents.

Furthermore, the rigorous privacy framework introduced by the GDPR initially led many to predict significant economic setbacks and a loss of competitiveness for EU businesses. However, subsequent research five years into the Regulation provides another point of view. Studies show how e-commerce professionals find the impact of GDPR minimal on their data-related processes and overall business operations[314]. In light of the Internet of Things (IoT) and big data's exponential growth, the informants even see GDPR as a necessary tool: if you provide a compliant and, therefore, trustworthy service, you have nothing to fear.

Web traffic serves as a useful benchmark in this context, reflecting the main consumer reactions to privacy measures. While there's an observable reduction in traffic, this decrease doesn't necessarily signify economic harm. Studies[315] suggest that users are

[311] *Ibid, "*One of the SMEs said the most significant benefit of GDPR was "getting things in order". "We had enough spreadsheets to fit in a football field" (P4). They moved everything onto the cloud, went paperless, slashed costs and reduced headcount by 2/3rd. In effect, GDPR meant "driving the digitalisation and automation of a lot of systems [. . .] and the restructure of the organisation" (P6)".
[312] GDPR, Art. 35(1).
[313] Ian Williams, '*Why DPIAs are a good thing'*, Articles on Linkedin, available at https://www.linkedin.com/pulse/why-dpias-good-thing-ian-williams/?trk=pulse-article
[314] Moutaz Haddaraa, Salazar, Ab, Marius Langsetha, *'Exploring the Impact of GDPR on Big Data Analytics Operations in the E-Commerce Industry'*, Procedia Computer Science 219 (2023) at 776.
[315] Raffaele Congiua, Lorien Sabatinoa, Geza Sapib, 'The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR', Information Economics and Policy 61 (2022) at 15; Sean Sirur, Jason R.C. Nurse, Helena Webb, '*Are we*

now more discerning, opting out of sites they deem intrusive. With GDPR necessitating clear informed consent for data collection, even reduced website visits could translate to net welfare gains[316], sidelining potentially harmful platforms in favour of those prioritizing safety. These results suggest that the regulation enhanced customer trust and confidence as well as business data security and management, benefiting all the environment on which companies operate.

Most of scholars share the idea for which these results stem from the fear of the hefty fines GDPR imposes on offenders. While this possibility clearly has prompted businesses to take privacy and security more seriously, it is important to stress how the purpose of GDPR was not to penalize businesses but to assist them in streamlining and organizing their data collection and handling procedures. In general, the regulation acted as a framework for developing the habits, principles, and experiences of those who work with data. Since then, businesses have grown to feel strongly that it is their responsibility to promote a culture that values data protection and respects the privacy of their customers. This resulted in the widespread[317] recognition that GDPR has been helpful in educating consumers about their rights and control over their data. Finally, there is no evidence of a negative effect of GDPR on the amount of content that EU digital creators/websites publish, nor on the average level of interaction and engagement with such content on social media[318] which remained stable. Paid search traffic – mainly Goodle advertisements – was barely affected as well[319], consolidating the idea that the only ones who may have been affected by the GDPR were smaller companies[320] unable to bear the costs necessary for their renewal. For the remainder, as seen in the paragraph, these costs proved to be minimal and/or profitable.

In sum, we can light-heartedly maintain that the analyzed advantages emerging from within the EU business landscape are not something to overlook. As seen, companies not only adapted but often thrived under the new framework, emphasizing robust data practices without compromising on their operational efficiency. Therefore, it is arguable that this adaptation and the subsequent benefits it brought forth didn't go unnoticed. In this sense,

---

there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)' ArXiv, (2018), at 3.

[316] *Ibid.*

[317] See Lisa Joy Rosner, '*GDPR: Bridging The Gap Between Consumer And Marketer Perceptions'*, Forbes Communications Council, Forbes, (2020).

[318] Vincent Lefrere, Logan Warberg, Cristobal Cheyre,Veronica Marotta, and Alessandro Acquisti, '*The Impact of the GDPR on Content Providers'*, (2020), at 1.

[319] Sean Sirur, Jason R.C. Nurse, Helena Webb, '*Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*', ArXiv, 2018, at 3.

[320] Raffaele Congiua, Lorien Sabatinoa, Geza Sapib, '*The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR'*, Information Economics and Policy 61 (2022) at 16;

non-EU observers began to see beyond the immediate challenges of compliance and instead of a mere regulatory burdensome hurdle to comply with, the GDPR was starting to be seen as a balanced model, efficiently harmonizing rigorous data protection with business needs. In the next paragraphs we will focus on how extensive GDPR's influence has actually been.

2.3 GDPR's influence worldwide

GDPR has prompted a global upsurge, pushing the topic of data privacy to the very forefront. Guidance regarding data subject rights, accountability requirements, and data breaches, all of which have greatly increased public interest in and awareness of how personal data is handled by organizations, is the part of the legislation that is most frequently being replicated globally.

Five years from its adoption, over one hundred countries[321] have put privacy standards in place, aligning themselves to the discipline set forth by the Regulation. While it is true that not all laws across other international laws are completely comparable to the GDPR, the majority do all share the same goal — giving individuals more control and ownership over their personal data. For instance, Canada's Personal Information Processing and Electronic Documents Act[322] (PIPEDA) now includes a Digital Charter that addresses cookies and opt-out options. In South Africa, the Protection of Personal Information Act[323] became fully operational in July 2020 and even the Privacy Act of Australia[324], which has been in effect since 1988, was recently updated to reflect GDPR requirements especially as to the concept of data controllers and processors[325]. The list goes on with several different countries such as Argentina, Brazil, Japan, Kenya, South Korea, and Chile[326] all pushing privacy standards at the base of their own regulations in the wake of GDPR, to the point that in some cases it is possible to talk about proper "legal transplants", a phenomenon addressed[327] by Alan Watson in 1973 (who coined the name) indicating the moving of a rule or a system of law from one country to another.

---

[321] Anthony Jones, '*The Global Impact of GDPR*' for Partners, 2022.
[322] Personal Information Protection and Electronic Documents Act, SC 2000, C5, https://canlii.ca/t/541b8 .
[323] Act. No.3 of 2013, Protection of Personal Information Act (POPI Act).
[324] Australian Act No. 119 of 1988, Privacy Act 1988, 14 December 1988.
[325] For an in-depth analysis of the alignment to GDPR from the Privacy Act, see this year's Privacy Act Review Report from PwC: https://www.pwc.com.au/cyber/cyber-updates/quick-guide-privacy-act-reforms_021623.pdf
[326] Supra Anthony Jones, '*The Global Impact of GDPR*'; Cask J. Thomson, '*Under Constant Supervision'*, BookRefine Publishing (2020), at 45.
[327] Alan Watson, '*Legal Transplants: An Approach to Comparative Law*', Second Edition, University of Georgia Press, Athens–London (1993).

As to Brazil, for instance, scholars[328] have referred to a legal transplant of the text of GDPR text, having it had a significant impact[329] even on the very initiative from Brazil to create specific data protection legislation, and thus inspired the text for the Brazilian General Data Protection Law[330] (LGPD or Law 13.709/18), which was signed into law on 14 August 2018. In comparison to Europe, where the first data protection laws were enacted decades ago, Brazil only recently entered into comprehensive discussions on data protection regulations, more precisely in 2009. Until then, the Brazilian data protection regulatory framework was sector-based and primarily governed by the country's Civil Rights Framework for the Internet (Internet Act), among other laws.

The legislation replicates key points of the European regulation, following the global trend of strengthening personal data protection, granting data subjects a number of rights, and imposing significant obligations and relevant penalties on processing agents. It does, however, include some Brazilian-specific features[331]. In contrast, the Brazilian law, like the GDPR, regulates controllers and processors of personal data[332] and establishes the principle of extraterritoriality, which means that the Law also applies to processors based outside Brazil that treat data collected in Brazilian territory or offer goods or services to individuals located in Brazil, regardless of where the organization is based.

In addition, non-compliance with the LGPD can have the same serious consequences as non-compliance with the GDPR. While EU enforcers can levy fines of up to 4% of global revenue, Brazil's system allows for fines of up to 2% of Brazilian revenue[333], with a cap of BRL 50 million (approximately USD 13 million or EUR 11,395.140) per violation.

In terms of enforcement, Law No. 13,853/2019 even establishes[334] the National Data Protection Authority ('NDPA'), which has the authority to: regulate data protection and privacy matters; impose administrative sanctions in the event of a violation of the LGPD

---

[328] See Renan Canaan Gadoni Canaan, '*The Effects on Local Innovation Arising from Replicating the GDPR into the Brazilian General Data Protection Law'*, Internet Policy Review, 12(1) (2023), at 5; Thiago Luís Sombra, '*The General Data Protection Law in Brazil: What Comes Next?'*, Global Privacy Law Review
Volume 1, Issue 2 (2020), at 116.
[329] Ius Laboris, '*The impact of the GDPR outside the EU',* Insights, (2019).
[330] Law No. 13.709 August 14, 2018, as amended by Law No. 13,853/2019 'General Personal Data Protection Act (LGPD)', available at https://lgpd-brazil.info
[331] *Ibid*. The main example is the legal base of the protection of credit allowing the processing of personal data, "specifically adapted to the needs of the credit sector in Brazil".
[332] LGPD, Chapter II, Artt. 7-16.
[333] LGPD, Art. 52.
[334] LGPD, Art. 55.

provisions; and propose guidelines for the creation of the National Policy for the Protection of Personal Data.

Despite the initial reluctance and the on-going inherent differences of approach, numerous States in the USA followed suit on the example provided from GDPR. One of the first state legislatures to adopt a broad-based, comprehensive privacy regulation similar to the GDPR was California. The California Consumer Privacy Act (CCPA)[335] of 2018 was passed in June 2018, just one month after the GDPR's deadline for enforcement. Only a week before it was approved, the CCPA was proposed, and it received unanimous support. The desire to protect constituents' data prevailed over usual partisan gridlock in a rare and encouraging turn of events. The CCPA, entered into effect in 2020, emphasizes consumer rights with regard to data at the point of collection.

While California led the states' efforts to enact data privacy and security laws, other states such as Vermont, Colorado and others swiftly followed by. Nevertheless, this still does not seem to drive toward the desired direction. In the USA, in fact, the call for GDPR-like privacy laws (and possibly at a federal level, avoiding state-by-state discrepancies) keeps increasing from both scholars[336] and businesses to the point that even Meta's owner Mark Zuckerberg has gone out on it.

In order to understand the reasons behind such demands, all the more important when it is also the most fined company under GDPR ever to make them (having Meta been sanctioned for a grand total of over 2.1 Billion Euros), we need to briefly recap the events which took place during the Cambridge Analaytica Scandal.

2.3.1. Cambridge Analytica and implications

On March 17, 2018, articles detailing how Cambridge Analytica obtained the personal information of over 50 million Facebook users and used it to try to boost support for the 2016 Trump campaign were simultaneously published in the Guardian[337] and New York Times[338]. The company's work had previously been reported, for instance, when US

[335] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199 (2018).
[336] *Inter alia*, see He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 22:1, 1-6, Michele E. Gilman, "*Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice,*" Arizona State Law Journal 52, no. 2 (2020), 368-444; Bernard Gallagher, 'Will the U.S. Adopt a Nationwide Data Privacy Law Similar to GDPR?', Partners, (2022).
[337] Guardian's Article https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[338] New York Times' Article https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Senator Ted Cruz used Facebook data in 2015[339]; however, the March revelations propelled the company to global attention, possibly as a result of the scope and any potential connections with the 2016 US presidential election and the Brexit referendum.

Before Steve Bannon left to become the CEO of the 2016 Trump campaign, Robert Mercer, a right-wing American billionaire, funded Cambridge Analytica, a consulting and data analytics firm that was led by him. The use of data by Cambridge Analytica to identify, target, and predict individual voters' voting intentions was covered in reporting. According to additional reporting, Cambridge Analytica helped the UK's Brexit campaign.

According to the Guardian and the New York Times, Facebook was aware that Cambridge Analytica had exploited its users' data by late 2015, but the company failed to notify those affected and engaged in limited and ineffective efforts to recover their data. Facebook later admitted that the number of people affected was far greater than what the Guardian and New York Times had initially reported: it had shared data from 87 million users.

The March 2018 story was neither the beginning nor the end as more information and questions have emerged in the years since, acknowledging that Cambridge Analytica's role was not limited to the United Kingdom and the United States: it took part in elections all over the world.

Certainly, the legal aftermath that followed these revelations was both immediate and extensive. In the United States, the Federal Trade Commission (FTC) fined Facebook a staggering $5 billion, part of a settlement that also required the social media giant to overhaul its user privacy practices. Alongside the FTC, the Securities and Exchange Commission (SEC) imposed a $100 million fine on Facebook for making "misleading disclosures" about the risks of user data misuse. State-level actions further compounded Facebook's legal woes. For example, attorneys general in Washington, D.C., and New York initiated their own investigations and lawsuits, alleging consumer protection violations. Class-action lawsuits filed by users accusing Facebook of breaching its fiduciary duty also added to the company's growing list of legal challenges.

Both Cambridge Analytica and Facebook became subjects of a rigorous parliamentary inquiry aimed at dissecting the complexities of disinformation and fake news.

[339] *See* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

In Canada, the Privacy Commissioner determined that both companies had violated Canadian privacy laws, adding yet another layer to their global legal challenges.

Beyond North America, the ripple effects of the scandal sparked investigations in other jurisdictions, including Australia and the European Union. As a follow up of the scandal, in fact, some MEPs demanded a full audit of Facebook and new anti-election meddling measures.

Sustaining that Facebook violated not only EU citizens' trust but also EU law, European Parliament issued a – non binding – Resolution[340] passed on the 25 October 2018 urging EU bodies to conduct a full audit to assess data protection and security of users' personal data. MEPs emphasized that Facebook should make changes to its platform in order to comply with EU data protection rules, as well as highlight the dangers of interference in democratic elections made possible by new technologies, proposing several measures to prevent said "meddling[341]". Subsequently, fines from the Italian DPA[342] and UK's ICO[343] would have been issued, respectively of 1 million Euros and 500.000£, the maximum under the Data Protection Directive. It is worth mentioning that had the GDPR been in force, having Facebook had earnings of €32.75 billion in 2017, it would have had to face a fine of over €1.3 billion).

Nonetheless, in light of the global scrutiny, Cambridge Analytica declared bankruptcy and ceased all operations in 2018. While the company itself may have shuttered, the legal and regulatory conversations it ignited are far from over as the case has become a linchpin in ongoing debates about data protection, having a long-lasting impact not just on the companies directly involved but on data privacy regulations and corporate responsibility globally.

---

[340] European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP))

[341] These included: applying conventional 'off-line' electoral safeguards online: rules on spending transparency and limits, respect for silence periods and equal treatment of candidates; making it easy to recognise online political paid advertisements and the organisation behind them; banning profiling for electoral purposes, including use of online behaviour that may reveal political preferences; that social media platforms should label content shared by bots, speed up the process of removing fake accounts and work with independent fact-checkers and academia to tackle disinformation; investigations should be carried out by member states with the support of Eurojust, into alleged misuse of the online political space by foreign forces.

[342] *Garante per la Protezione dei Dati Personali*, Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. - 14 giugno 2019 [9121486], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121486

[343] *Information Commissioner's officer*, fine resulting from the investigation available at https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

Most of all, the scandal serves as an example of how privacy is also about a person's autonomy, dignity, and right to self-determination and is a necessary prerequisite for democracy[344]. Since then, it has become a linchpin in ongoing debates about data protection, having a long-lasting impact not just on the companies directly involved but on data privacy regulations and corporate responsibility globally. The shortly-after entering into force GDPR appears to take all of this into account and companies recognize it.

2.3.2. The Meta Case: Mark Zuckerberg striving for GDPR-like regulations

Given that Meta Platforms Inc. bears the brunt of enforcement, constituting an astonishing majority—over 50 percent—of the total $4 billion in GDPR fines to date, one might reasonably assume that the company's CEO and founder, Mark Zuckerberg, harbors a negative view of the regulation. Contrary to such expectations, however, this is not the case.

After the events of Cambridge Analytica and the consequent backlash, Meta's Chairman explicitly demanded for new privacy regulations worldwide modelled on the European's GDPR. During an interview with the Washington Post[345], in fact, Zuckerberg began by notably expressing his support for more active government and regulatory intervention. He argued that updating the rules governing the internet could strike a balance between preserving individual freedoms—such as free expression and entrepreneurial innovation—and mitigating societal harms. The best way to do so is following GDPR's steps:

"*Effective privacy and data protection needs a globally harmonized framework. People around the world have called for comprehensive privacy regulation in line with the European Union's General Data Protection Regulation, and I agree. I believe it would be good for the Internet if more countries adopted regulation such as GDPR as a common framework.*

Zuckerberg then proceeds to double down on his (and our) view, for which the balancing enacted by the Regulation beneficiates everyone: "*New privacy regulation in the United States and around the world should build on the protections GDPR provides. It*

[344] Privacy International, 'Cambridge Analytica, GDPR - 1 year on - a lot of words and some action', (2019), https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action

[345] Mark Zuckerberg, 'The Internet needs new rules. Let's start in these four areas' Opinion for the Washington Post, (2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html#

should protect your right to choose how your information is used — while enabling companies to use information for safety purposes and to provide services".

In conclusion, the aspiration for a unified global framework for data protection seems to be a shared goal, with the GDPR serving as a potential blueprint for such harmonization. Mark Zuckerberg's nuanced take on GDPR seems to echo this sentiment, advocating for more clarity in rules and a role for governance in tackling the ethical dimensions of emerging technologies like artificial intelligence.

Such a stance lends weight to the notion that GDPR, while often criticized, has emerged as the most robust and balanced framework for data protection currently available. Although not without its imperfections, the regulation accomplishes the complex task of safeguarding individual privacy rights while not stifling economic activity. Moreover, it sets a precedent for how emerging technologies should be responsibly managed and governed. Mark Zuckerberg's perspective validates the broader industry acknowledgement that the GDPR serves as a promising model for both businesses and policy experts alike. It not only sets the standard for individual data protection but also provides an environment conducive to technological innovation in a safe, controlled way.

Clearly, wide margin for improvement remains, as the same Chairman of Meta points out in his opinion[346], especially on hot topics like emerging technologies. When tackling technology, policymakers must look forward, and the Regulation does leave some space for integration when looking in perspective which will hopefully be filled by the upcoming legislation in the data protection framework. Our final analysis of this thesis will focus specifically on this.

3. GDPR and emerging technologies, addressing the challenges

[346] *Ibid*. In closing his opinion, Zuckerberg states:'*As lawmakers adopt new privacy regulations, I hope they can help answer some of the questions GDPR leaves open. We need clear rules on when information can be used to serve the public interest and how it should apply to new technologies such as artificial intelligence'.*

Researchers have long agreed that technology advances are accelerating at a rate that legal frameworks cannot keep up with[347]. For legislators, therefore, the challenge extends beyond just satisfying the immediate needs of data subjects and controllers. They must also deal with the relentless pace of technological innovation, which risks rendering any regulatory framework obsolete almost as soon as it comes into force. Thus, the ongoing task for lawmakers is to construct a regulatory environment that can both protect individual privacy and accommodate the ever-changing state of technology.

Although the difficulties and complexities of digital environments were considered when developing the data protection regulatory strategy, the regulatory choice in GDPR consisted in what scholars[348] perceive as "technology-independent legislation." This entails a deliberate absence of technology-specific terminology and provision that can be attributed to the "technological neutrality approach" explicitly established in Recital 15.

Technology-independent rules are regarded as a means of remaining stable in the midst of technological turbulence[349] where the emphasis is put not on the technology used for data processing, but on the effects that must be regulated, on the risks and impacts on fundamental rights that must be faced. While adopting technology-neutral provisions appears to be the best way[350] to deal with the unpredictability of technological developments and, as a result, ensure that the law is long enough to respond successfully to such - unpredictable – developments, we argue that while emphasizing general principles and effects over specific technological details can enhance regulatory flexibility, it may introduce some uncertainties and challenges, particularly in the context of innovative tech developments. When it comes to emerging technologies the GDPR has admittedly functioned as both guidance and regulatory challenge for their integration, as the principles at the very core of the Regulation enshrined in Article 5 do collide with some of the ground-level necessities of these technologies.

In our analysis, we will specifically address cloud computing, blockchain, the Internet of Things, and artificial intelligence: these technologies have gotten a lot of attention

[347] On the topic, see Nir Kshetri, '*Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution',* Telecommunications Policy 37, no. 4–5 (2013), 372-386; Robert Herian, '*Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty.*' Journal of Internet Law 22, no. 2 (2018), 8–16; Mira Burri, and Rahel Schär. '*The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy'*, Journal of Information Policy 6, no. 2016 (2016).
[348] Lilian Mitrou, '*Is the General Data Protection Regulation (GDPR) "artificial intelligence*-proof" ?', Tilburg: TILT Law & Technology Working Paper Series (2018), at 26.
[349] Bert-Jaap Koops, '*Should ICT Regulation be Technology-Neutral? Starting points for ICT regulation. Deconstructing prevalent policy one-liners*', IT & Law Series (eds.), Vol. 9, (2006), at 1.
[350] *Supra* Lilian Mitrou.

from researchers and industry in very recent times as they foster innovation in both public and private companies, but they also threaten individuals' privacy[351].

Moreover, these technologies all share a common characteristic, this being an openness that makes them remarkably innovative[352]. We argue that some of the Regulation's principles, (mainly, as we will see, data purpose limitation and minimization) call into question the inherent properties of these technologies.

3.1 Internet of Things

Recent advancements in hardware and information technology have accelerated the proliferation of smart and interconnected devices, allowing the Internet of Things (IoT) to develop at a rapid pace. IoT applications and services are widely used in areas such as smart cities, smart industries, self-driving cars, and eHealth. As a result, IoT devices are everywhere connected, constantly transferring sensitive and personal data without the need for human intervention and feeding, therefore, data protection concerns.

A comprehensive definition of IoT describe it as "the interconnection of sensing and actuating devices that enables the sharing of information across platforms via a unified framework, developing a common operating picture for enabling innovative applications. This is accomplished through the use of seamless ubiquitous sensing, data analytics, and information representation, with cloud computing serving as the unifying framework[353]."

IoT provides numerous benefits to organizations and nations, including increased productivity, improved quality of life, process automation, personalization of services, context-specific applications, and real-time data generation[354]. However, there are significant issues that impede the realization of those values, such as privacy, security attacks, interoperability due to device heterogeneity, technological immaturity in storing and processing massive amounts of data, and insufficient regulatory frameworks[355].

---

[351] Rania El-Gazzar, Karen Stendal, '*Examining How Gdpr Challenges Emerging Technologies'*, Journal of Information Policy, Volume 10, (2020), at 237.
[352] See Michel Avital, '*Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future'*, Proceedings of the 37th International Conference on Information Systems, (2016) at 3.
[353] Jayavardhana Gubbi, et al. '*Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions'* Future Generation Computer Systems 29, no. 7 (2013), at 1647.
[354] For an in-depth analysis, see Papadopoulou Panagiota, '*Investigating The Business Potential Of Internet Of Things'* MCIS (2017) Proceedings, Genoa, Italy, Association for Information Systems, (2017) 1-12.
[355] *Ibid.*

With 15.6 billion devices connected as per 2023[356] (2 connected objects per person), data privacy in Internet of Things (IoT) and an expected increase by around 12 percent per year[357], the Internet of Things presents exceptional challenge for regulation bodies. To this extent, determining the (multi-dimensional) GDPR's impact presents as quite a difficult task as IoT systems can achieve a great degree of complexity[358]. However, some key aspects must be considered when determining how the GDPR applies to an IoT system.

Authors share the idea for which[359] GDPR poses some challenges for IoT, which outstandingly vast amount of data collection clashes with the discipline laid down for consent and most of all in regard to security and accountability. According to the Article 29 Data Protection Party ("WP 29"), Internet of Things (IoT) entails extensive processing of a massive amount of data collected on identifiable natural persons via sensors and processes this data to analyze the individual's environment or behavior[360]. This collection of voluminous personal data is likely to contain more information than is required, from data subjects or sensors in IoT devices through automated invasive tracking of data subjects' behavior[361].

Similarly, third parties involved in the processing of personal data may use the data for purposes unknown to the data subject[362]. This violates the GDPR's data minimization principle, which states that data must be relevant and limited to what is required for the purposes for which it is collected[363]. Controllers will comply with GDPR if they limit the amount of personal data collected by IoT devices, but the IoT services will not function properly[364]. This implies that if personal data collection is minimized, the business model for using IoT services is no longer adequate. Furthermore, using inferences for purposes other than the intended data collection purpose and without the consent of the data subject violates the GDPR's purpose limitation principle[365].

---

[356] Number of IoT Devices (2023), https://explodingtopics.com/blog/number-of-iot-devices#
[357] Number of connected IoT devices will surge to 125 billion by 2030, (https://electroiq.com/2017/10/ number- of-connected- iot- devices- will- surge- to- 125- billion- by- 2030/).
[358] Ombir Sharma, '*How Does GDPR Impact Emerging Technologies*?', Data and Technology Insights, (2022).
[359] Adam Finlay, Ruairì Madigan, '*GDPR and the Internet of Things: 5 Things You Need to Know'*. Retrieved, (2017), 1-2; Lilian Edwards, '*Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*' Forthcoming European Data Protection Law Review, (2016), at 36.
[360] Working Party 29, Opinion 8/2014, page 4.
[361] See Sandra Wachter '*Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR',* Computer Law and Security Review 34, no. 3 (2018), at 2.
[362] *Ibid,* at 11.
[363] GDPR, Art. 5(1)c.
[364] *Ibid.*
[365] GDPR, Art. 5(1)b.

Furthermore, IoT is also distinguished by the use of big data analytics as well as complicated algorithms to make invasive profiling inferences about the data subject by linking IoT datasets or combining datasets shared by third parties[366], which sheds lights on other – similar – issues.

3.2 GDPR and the processing of Big Data

Big data refers to large or complex volumes of structured and unstructured data that can be analyzed to provide value. It is typically[367] defined by a number of V-properties, namely velocity, volume, value, variety and veracity. Today, big data has become capital, with businesses significantly improving their operations and customer relations and academia developing and improving research[368].

While the utility of big data processing is undeniable, it also poses significant privacy risks when dealing with personal information. This is due primarily to two aspects of big data analysis. First, the greater the amount of data, the greater the likelihood of re-identifying individuals, even in datasets that appear to lack personal linking information. Second, big data analysis can infer new information from "harmless" personal data that was not intended to be revealed by the affected person.

When it comes to GDPR, data which lacks identifiers is commonly regarded as anonymous and falls outside the scope of the GDPR[369].Big data analysis results are frequently statistical findings with no direct links to specific individuals. As a result, processing only anonymous data is a simple way to meet all GDPR requirements. The definition of anonymity, on the other hand, is not so simple. Even if directly identifiable parameters are removed from a dataset, combining the dataset with other information may allow single individuals to be re-identified[370].

---

[366] Sandra Wacther, '*The GDPR and the Internet of Things: A Three-Step Transparency Model'* Law, Innovation and Technology 10, no. 2 (2018b), at 283.

[367] Inter alia, Gartner IT Glossary, '*What Is Big Data*?' (2018); Thuan Nguyen, '*A Framework for Five Big V's of Big Data and Organizational Culture in Firms',* 2018 IEEE International Conference on Big Data (Big Data), (2018) at 1; Burt Monroe '*The Five Vs of Big Data Political Science Introduction to the Virtual Issue on Big Data in Political Science*' Political Analysis. 21(V5) (2013), at 1; Surya Gutta, '*The 5 V's of Big Data'*, Medium, (2020); Gayatri Kapil, Alka Agrawal and Raees Ahmad Khan, '*A study of big data characteristics'* International Conference on Communication and Electronics Systems (ICCES), (2016), at 2.

[368] Gruschka, Nils & Mavroeidis, Vasileios & Vishi, Kamer & Jensen, Meiko. (2018) '*Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR'*, Conference: 2018 IEEE International Conference on Big Data (Big Data) (2018), at 1.

[369] GDPR, Recital 26.

[370] This process is also referred to as background knowledge attack; for a deeper focus, see Ashwin Machanavajjhala, Muthuramakrishnan Venkitasubramaniam, Daniel Kifer, and Johannes Gehrke, '*L-Diversity: Privacy Beyond k-*

The GDPR does not directly address the terms big data or data analysis. However, as it is presumable from the introduction, big data and the GDPR are not always compatible[371], being big data analytics opposed – almost by definition - to the data minimization principle[372]. The rush to Big Data creates a clear incentive for businesses to collect and retain as much data as possible for as long as possible (while accounting for the non-trivial costs of data collection and analysis). Big data mining, for example, is based on the analysis of large amounts of data, which frequently contradicts the principle of data minimization.

Furthermore, new hypotheses for testing are frequently introduced after the data has been collected in data analysis. However, the data subjects from whom the data were collected initially provided consent for a different purpose. Thus, from a legal standpoint, data processing should be done on anonymized data whenever possible; otherwise, great care must be taken to ensure that the GDPR is followed. Under Art. 35, this may necessitate a data protection impact assessment (DPIA) which, as we have seen, is necessary to identify and analyze how certain actions or activities may affect data privacy[373].

As many reports have pointed out[374], the principle of purpose specification enshrined in Article 5(1)(b) is clearly at odds with the prospect of Big Data analyses as well. A lot of the time, analyzing Big Data involves methods and usage patterns that neither the entity collecting the data nor the data subject considered or even imagined at the time of collection." To comply with the purpose specification rule, entities attempting to engage in Big Data analysis will need to inform their data subjects of the future forms of processing they will engage in (which must still be legitimate by nature) and closely monitor their practices to ensure they did not exceed the permitted realm of analyses. In sum, carrying out any of these tasks could be costly, difficult, or even impossible[375].

Anonymity', in 22nd International Conference on Data Engineering (ICDE), (2006), at 24; Daniel Kifer and Ashwin Machanavajjhala, '*No free lunch in data privacy'*, International Conference on Management of Data (2011), 193.

[371] Tal Z. Zarsky, '*Incompatible: The GDPR in the Age of Big Data'*, Seton Hall L. Rev., vol. 47, (2016), at 996.

[372] Colin J. Bennett, Robin M.Bayley, '*Privacy Protection in the Era of Big Data*', Regulatory Challenges and Social Assessments, Chapter in 'Exploring the boundaries of big data' Bart van der Sloot, Dennis Broeders & Erik Schrijvers (eds.), (2016) at 210; Antoinette Rouvroy, "Of Data and Men ": Fundamental Rights and Freedoms in a World of Big Data, (2016), at 14.

[373] GDPR, Art. 35.

[374] See, Mireille Hildebrandt, '*Slaves to Big Data. Or Are We*?', IDP. REVISTA DE INTERNET, DERECHO Y POLITICA? 16, 17 (2013); Bart van der Sloot, Sascha van Schendel, '*Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*', 7 JIPITEC29 (2016), at 38-39.

[375] Supra Tal Z. Zarsky, *'Incompatible: The GDPR in the Age of Big Data'*, at 1005.

3.3 Blockchain

Blockchain consists in a distributed, immutable ledger that stores and shares the entire previous transaction history in a series of blocks in a public ledger between distributed computers on a network[376]. Every time a transaction is changed, a new block is created and validated by the participating nodes; if consensus is reached, the newly generated block is chained to the previous blocks[377]. All transactions are timestamped, and their history is permanently saved and distributed to all participants[378]. Transparency, immutability (i.e., a tamper-proof ledger of transaction history), and deployment models (i.e., public permissionless and private permissioned[379]) are the main characteristics of BC. This system renders the number of users who can process and read transaction data in public permissionless blockchains basically unlimited and stands, of course, in inherent tension with the mentioned guiding principles of GDPR.

The very reason of success of the blockchain, this being its immutability (that means the data can never be changed or deleted), in fact, clashes with several different guiding principles of the Regulation. The immutability of public permissionless blockchains contradicts the GDPR's right to erasure[380] and right to rectify incorrect data[381] granted to data subjects[382]. Furthermore, the ever-growing immutable ledger of transaction history in blockchain[383], particularly in public permissionless blockchains, raises concerns about GDPR's storage limitation principle[384] and, at the same time, conflicts with data minimization principle[385] as the requirement for data to be widely distributed clashes with

[376] Lindman, Juho, Matti Rossi, and Virpi Kristiina Tuunainen. 'Opportunities and Risks of Blockchain Technologies in Payments– A Research Agenda' Proceedings of the 50th Hawaii International Conference on System Sciences, Maui, HI, ScolarSpace, (2017), at 1533.
[377] See Korpela, Kari, Jukka Hallikas, and Tomi Dahlberg. '*Digital Supply Chain Transformation toward Blockchain Integration*', Proceedings of the 50th Hawaii International Conference on System Sciences 41 (2017) at 4185.
[378] Alexopoulos Charalampos, '*Benefits and Obstacles of Blockchain Applications in E-Government'*, Proceedings of the 52nd Hawaii International Conference on System Sciences, (2019), at 3378.
[379] For a deeper analysis, see Sarah Underwood, '*Blockchain Beyond Bitcoin*' Communications of the ACM 59, no. 11 (2016), 15–17; Makhdoom Imran, '*Blockchain's Adoption in IoT: The Challenges, and a Way Forward'* Journal of Network and Computer Applications 125, no. 2019 (2019): 251–79.
[380] GDPR, Art. 17.
[381] GDPR, Art. 16.
[382] See David Hawig, '*Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation-Compliant Health Data Exchange: A Use Case in Blood Glucose Data'* Journal of Medical Internet Research 21, no. 6 (2019).
[383] See supra, Sarah Underwood, '*Blockchain Beyond Bitcoin'*.
[384] GDPR, Art. 5(1)e.
[385] GDPR, Art 5(1)c.

the need of a processing that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

While GDPR is built on a foundation that emphasizes user control over personal data, blockchain's architecture is geared toward irreversible, transparent record-keeping. As a result, once data is written in the blockchain, it cannot be erased. Any modification to a single block has the potential to invalidate subsequent blocks. Moreover, people who share their data on the blockchain can have access to the shared data and see how it is processed without any obstacles.

GDPR's accountability principle[386] is even more burdensome as this rule assumes the existence of a controller, and many blockchains strive for decentralization. The question of who is responsible for data controllers is basically impossible to answer: anyone who joins the network and runs software can access the network in a distributed ledger system. This means that anyone with network access becomes a data controller. Both legal studies[387] and scholars[388] have presented possible solutions. Nevertheless, there is no verified and flexible solution to this kind of problem, so the growth of blockchain has slowed[389]. Even if one could create a blockchain that adhered to the presented GDPR principles and defend their work, it would ultimately be impossible to reconcile the blockchain with Article 17 of the GDPR—the right to erasure, also known as the right to be forgotten[390].

3.4 Cloud

The US National Institute of Standards and Technology (NIST)[391] defines Cloud as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Cloud models divide into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)[392]and customers do not

[386] GDPR, Art. 5(2)
[387] See Ombir Sharma, '*How Does GDPR Impact Emerging Technologies*?', CMS law solution.
[388] See Mateusz Godyn, Michal Kedziora, Yingying Ren, Yongxin Liu, Houbing Herbert Song, '*Analysis of solutions for a blockchain compliance with GDPR'*, Scientific Reports 12, 15021 (2022).
[389] Bahalul Haque, Najmul Islam, Sami Hyrynsalmi, Bilal Naqvi, Kari Smolander, '*Gdpr compliant blockchains—a systematic literature review'*, IEEE Access (2021), 5 (2021), at 50604.
[390] Diogo Duarte '*An introduction to block chain technology from a legal perspective and its tensions with the GDPR'*, Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law (2019), at 43.
[391] Peter Mell, and Timothy Grance '*The NIST Definition of Cloud Computing'*, Association for Computing Machinery. Communications of the ACM, (2010), at 2.
[392] Ibid.

manage or control the cloud infrastructure in any of the three, but they do have limited control over the configuration settings. The NIST definition of cloud computing conveys the technical characteristics of cloud computing, these being elasticity, pooled resources, on-demand access, self-service, and pay-as-you-go.

These unique features provide many benefits to organizations which increased efficiency in services provided and technological innovation[393] as a result. However, this flexibility also poses GDPR-specific privacy and security challenges. As seen, unlike previous privacy legislation, GDPR has distinct requirements for both data controllers and data processors[394]. In cloud computing, the precise identity of the data controller and data processor is complicated and depends on the actual data processing agreement and the types of cloud computing services. For example, a Software as a Service (SaaS) provider typically provides services intended to process data as the controller, but the SaaS provider may also control the purpose of the data and the means of processing it. In this case, the SaaS provider serves as both data controller and data processor[395].

A provider of Infrastructure as a Service (IaaS), on the other hand, provides virtualized cloud computing infrastructure and only processes data on behalf of users. The users of the IaaS service act as data controllers, determining the purpose and method of data processing[396]. Prior to GDPR, data controllers bore the majority of the burden of data privacy protection and local data law compliance. In contrast, data processors now face the same legal obligations to protect personal data as data controllers under GDPR.

Moreover, nowadays Cloud services are used by companies and organizations of all types and sizes which often process multitudes of common and/or 'sensitive' personal data of users who may sometimes be vulnerable subjects such as minors. Under the Regulation's accountability principle, cloud providers are required to demonstrate compliance, implying that a GDPR compliance solution should keep tamper-proof evidence for the massive data processing activities in cloud services[397]. For this reason, the data controller must carefully choose the cloud provider, taking into account the principle of accountability whereby the

[393] Lei Gao, Kevin Eller, Austin F. Eggers '*GDPR and the cloud: examining readability deficiencies in cloud computing providers'* Privacy Policies, Policy Studies (2022), at 8.
[394] Mark Webber. '*The GDPR's Impact on the Cloud Service Provider as a Processor'* Privacy & Data Protection 16 (4), (2018) at 1.
[395] Supra Lei Gao, Kevin Eller, Austin F. Eggers, '*GDPR and the cloud: examining readability deficiencies in cloud computing providers*' *privacy policies'*.
[396] Mirsolav Chlipala, Stefan Pilar, *'Cloud Service Provider – Processor, Controller Or Both?'*, INPLP (2017).
[397] *See* Chen Zhou, Masoud Barati, Omair Shafiq, '*A compliance-based architecture for supporting GDPR accountability in cloud computing'*, Future Generation Computer Systems,Volume 145, (2023), Pages 104-120.

controller not only has to comply with all the Privacy legislation (i.e. not only GDPR, but also national legislation and the opinions of the competent Authorities), but also to prove it. This principle also means that the data controller must be 'proactive' in complying with the legislation in the sense that it must do everything possible, taking into account its organisation, costs and the state of the art, to put in place appropriate technical and organisational measures.

GDPR also requires data processors, including cloud computing providers, to develop formal procedures to protect personal information in the event of a breach. In sum, the complexity of identifying data processors and data controllers in cloud computing, combined with the additional legal responsibilities imposed by GDPR, may expose cloud computing service providers to extensive litigation risks.

3.5 GDPR and AI

In completion of the emerging tech analysis and concluding the Chapter, a focus must be given to Artificial Intelligence and its space in the GDPR. The technical definition of AI is based on the concept of the "intelligent" machine, which "perceives its environment and takes actions that maximize its chances of success at an arbitrary goal"[398]. The ability to predict and anticipate possible future events based on data analysis to model some aspect of the world is proposed as a definition to codify and/or indicate not only the characteristics but also the expectations from AI[399]. This point is made very clear in the US AI report[400], which defines AI as a technology that, when used thoughtfully, can help to augment human capabilities rather than replace them.

GDPR makes no mention of AI. Although the difficulties and complexities of digital environments were considered when developing the data protection regulatory strategy, in this thesis we have already argued how the absence of technology-specific terminology and provisions appears to be a deliberate choice. This approach has also been referred to as "technological neutrality approach"[401] and stems from the explicit adherence from European

[398] Stuart Russell and Peter Norvig, *'Artificial Intelligence: A Modern Approach'* (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, (2003), at. 23.
[399] UK Government Office for Science, '*Artificial intelligence: opportunities and implications for the future of decision making*', (2015), p. 5.
[400] White House Office of Science and Technology Policy (OSTP), *Preparing for the Future of Artificial Intelligence,* (2016).
[401] Supra Lilian Mitrou, '*Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof"*' ?', at 26.

legislators enshrined in Recital 15 citing that the protection of natural persons should be technologically neutral and should not depend on the techniques used.

Nevertheless, GDPR applies to the development of artificial intelligence as well as its use for analyzing and making decisions about individuals[402]. The provisions concerning the scope of application, the legal grounds, the data protection principles, and automated decision-making are particularly relevant in the AI-environment.

When combined with AI, previously identified Big Data tendencies apply with enhanced implications for data processing and protection. There is a tension between the traditional data protection principles - purpose limitation, data minimization – and the full deployment of the power of AI and big data. These tendencies primarily refer to the collection of "all data" or "as much data as possible" in order to learn and analyze more effectively[403] as well as the re-purposing or multi-purposing of data and the consequent clash with the purpose limitation principle. With AI, in fact, data generated in a specific context and/or activity can be used and analyzed for a previously unknown and broad range of purposes. AI basically enables the harvesting and harnessing of massive amounts of data, as well as its repurposing and, as our current analysis on emerging technology and scholars suggest if the processing does not satisfy the purpose limitation principle then it is presumable that it will not satisfy the data minimization principle as well and vice versa[404].

The challenge for data controllers, therefore, becomes defining from the start the purposes of the processing, which is difficult to answer because it is impossible to predict what the algorithm will learn, and the data that will be relevant, thereby limiting the amount of data included in training or in the use of a model[405]. The data minimization principle, in this context, refers to both the volume of data and the processing activity. In this context, the data minimization principle refers to both the volume of data and the processing activity. Compliance with the data minimization principle may limit the extent of an individual's (informational) privacy intervention or even lead to the avoidance of the use of AI

[402] See Paul Niemitz, '*Constitutional Democracy and Technology in the age of Artificial Intelligence'*, Royal Society Philosophical Transactions, (2018).
[403] To this end, see the Norwegian Data Protection Authority emphasizes the increased demand for data. See Danish DPA Datatilsylnet, Artificial Intelligence and Privacy -Report, 2018, at 11.
[404] See Marcel Butterworth, '*The ICO and artificial intelligence: The role of fairness in the GDPR framework'*, Computer Law & Security Review, Volume 34, Issue 2, 2018, at 260; *supra* Lilian Mitrou, '*Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof*"' at 50.
[405] Supra Danish DPA, at 18. The Norwegian Authority pointed out that "*it would be natural to start with a restricted amount of training data, and then monitor the model's accuracy as it is fed with new data".*

models/methods if the processing goal can be achieved in a less invasive way for the individuals' privacy.

Finally, Artificial intelligence-powered systems whose decisions cannot be explained raise fundamental issues of accountability[406]. Compliance entails, among other things, the controller being able to explain how personal data processing was implemented and how a specific decision was reached. Responding to accountability requirements in the AI environment appears to be a difficult task, given the opacity of processing and the use of algorithms that lack a decision tree structure and rely on the analysis of large amounts of data to establish correlations. for outcomes as well as accountability for massive amounts of personal data[407]. The requirements of this new principle have a number of ramifications for organizations engaged in big data analytics and/or machine learning. In this context, accountability entails checking and demonstrating that the algorithms developed and used by machine learning systems "are actually doing what we think they're doing and aren't producing discriminatory, erroneous, or unjustified results"[408].

Overall, The GDPR permits the development of AI and big data applications that successfully balance data protection and other social and economic interests, but it provides little guidance on how to do so[409]. Hence, the effective implementation of GDPR to AI-application is heavily reliant on the guidance provided by data protection bodies and other competent authorities to controllers and data subjects[410]: appropriate guidance would reduce the cost of legal uncertainty and direct businesses, particularly small businesses, to efficient and data protection-compliant solutions. A fitting example is provided by the very recent case between OpenAI and the Italian DPA.

3.6 How to achieve compliance: ChatGPT and Italian DPA's data-block guidance

ChatGPT, which stands for "Chat Generative Pre-trained Transformer," is an AI-driven Virtual Assistant created by OpenAI, a well-known artificial intelligence research

[406] See 40th International Conference of Data Protection and Privacy Commissioners, 'Declaration on ethics and data protection in Artificial Intelligence', (2018), Brussels.
[407] See Giovanni Buttarelli, 8th Annual Data Protection and Privacy Conference Brussels, 30 November 2017 Keynote speech.
[408] Information Commissioner Office (ICO), '*Big data, artificial intelligence, machine learning and data protectio*n', 2017, par. 113.
[409] European Parliamentary Research Service (EPRS), '*The impact of General Data Protection Regulation on Artificial Intelligence*', Scientific Foresight, (2020), Intro at III.
[410] *Ibid.*

organization. ChatGPT, which functions as a language model, is meant to participate in realistic conversations with humans, offering users with an experience similar to conversing with a real person, capable of providing insights on a quasi-infinite range of subjects. ChatGPT belongs to the “generative" category of artificial intelligence, a subset that focuses on generating new material, such as pictures, text, or audio, by using patterns and examples obtained from existing data.

On March 30, 2023, the Italian Data Protection Authority, known as the Garante per la protezione dei dati personali, in line with its corrective powers under Article 58[411] issued an interim order[412] requiring the US-based company Open AI LLC to temporarily halt the processing of personal data belonging to individuals in Italy using ChatGPT. The Garante’s decision admittedly created a sensation among scholars, being addressed as the most headline-grabbing action by a data protection authority in the AI space to date because of its impact on ChatGPT, which is reportedly the fastest growing consumer application in history[413].

While the decision was prompted by a data breach concerning users' conversations and payment information of subscribers to the paid service, the DPA reported the lack of information to users and all those whose data is collected by OpenAI, but above all the absence of a legal basis justifying the massive collection and storage of personal data for the purpose of 'training' the algorithms underlying the platform's operation. The Garante also lamented that the processing of personal data of interested parties was inaccurate as the information provided by ChatGPT does not always correspond to the real data as well as the absence of any verification of the users' age in relation to the ChatGPT service which, according to the terms published by OpenAI, is reserved for individuals who are at least 13 years old. In light of the above, the Garante concluded that the processing of users' personal data, including that of minors, by ChatGPT was in violation of Articles 5, 6, 8, 13 and 25 of the GDPR.

On 6 April 2023, the Garante announced[414] that, during a meeting, OpenAI confirmed its willingness to cooperate in order to address the Garante's concerns about ChatGPT, while

[411] GDPR, Art.58(2)f grants the possibility to impose a temporary or definitive limitation including a ban on processing to every supervisory authority.
[412] GPDP, Provvedimento del 30 marzo 2023, available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870832
[413] Pietro Altomani, ‘*Italian Garante bans Chat GPT from processing personal data of Italian data subjects’*, Data Protection Report, (2023).
[414] GPDP, ‘ChatGPT: OpenAI collabora con il Garante privacy con impegni per tutelare gli utenti italiani’, Comunicato stampa, (2023), available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9872832

also outlining that OpenAI believes it is complying with applicable personal data protection laws. The Garante reported, in particular, that OpenAI is committed to increasing transparency in the use of data subjects' personal data, as well as existing mechanisms for exercising data subject rights and safeguarding children. Furthermore, the Garante stated that OpenAI had agreed to provide a document outlining the steps taken to address the Garante's requests. Only six days later, the Garante announced[415] that OpenAI's deadline to comply with the DPA's requirements and thus obtain a halt to the temporary ban imposed on OpenAI to process the personal data of Italian data subjects was due to 30 April 2023. Compliance would have allowed ChatGPT to be available from Italy once more.

Finally, on April 28, 2023, the DPA announced[416] that it had received a letter from OpenAI outlining the measures the latter had taken in order to comply with the Garante's order. The Garante specifically mentioned that OpenAI, among other things, expanded the information provided to EU users and non-users. It amended and clarified several mechanisms and deployed solutions to enable users and non-users to exercise their rights, such as the right to opt-out of processing of personal data for algorithm training. OpenAI also added a button to a dedicated page reserved for Italian registered users that allows them to confirm that they are at least 18 years old before gaining access to the service, or that they are over 13 and have obtained parental consent. Following suit of the letter, the Garante authorized the reinstatement of ChatGPT for Italian users.

4. GDPR as a standard. Some conclusive remarks

The Garante's case against OpenAI showcases how emerging technologies, with their significant data processing demands, can indeed pose challenges within the existing data protection framework. What also emerges, on the other hand, is that the Regulation and emerging technologies are not inherently conflicting and can be aligned to ensure coexistence through businesses' commitment.

[415] GPDP, '*ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola*' , Comunicato stampa, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751#english

[416] GPDP, '*ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei',* Comunicato stampa, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490

Businesses that use these technologies must ensure that their standards are in line with the regulations, making transparency essential for GDPR compliance. Increasing transparency could reveal outstandingly beneficial: companies that are open and honest with their customers about how they use their data will be in a much better position to respond to complaints and avoid fines[417].

In IoT, study finds that the major issues registered with GDPR are indeed caused by a lack of transparency, followed by consent, privacy, discrimination, and complex contractual relationships[418], making accountability all the more important. This is corroborated from scholars, who find that the need for accountability in the IoT is motivated by the opacity of distributed data flows, insufficient consent mechanisms, and a lack of interfaces allowing end-user control over the behavior of Internet-enabled devices[419]. The lack of accountability would preclude meaningful engagement by end users with their personal data and is a major barrier to building user trust in IoT and the reciprocal development of the digital economy[420].

A good example is provided by blockchain which is by-default transparent, manifesting an auditable distributed ledger of transaction data and history that is easily accessible to all the participants of the blockchain (i.e., individuals or other bodies with controller or processor responsibilities or both)[421]. This makes blockchain compliant with the GDPR principles of lawfulness, fairness, and transparency[422], where transparency requires that any information and communication relating to the processing of personal data be easily accessible and understandable, and that clear and plain language be used to ensure fairness and transparency. The transparency of blockchain also improves accountability by tracking all transactions[423], allowing compliance with the GDPR accountability principle, which is clearly non-negotiable. In this sense, it does not come as a surprise that transparency is an explicit key priority[424] of the recently approved EU AI Act[425], the first global regulation

[417] Supra Ombir Sharma, '*How Does GDPR Impact Emerging Technologies?*', at 10.
[418] Supra Rania El-Gazzar, Karen Stendal, '*Examining How Gdpr Challenges Emerging Technologies'*, at 258.
[419] Lachlan Urquhart, Tom Lodge and Andy Crabtree, '*Demonstrably doing accountability in the Internet of Things'*, International Journal of Law and Information Technology, (2019), 27, at 1.
[420] *Ibid*.
[421] Michèle Finck, *'Blockchain and the General Data Protection Regulation Can Distributed Ledgers Be Squared with European Data Protection Law*?' (2019).
[422] *Supra*, Rania El-Gazzar, Karen Stendal, '*Examining How Gdpr Challenges Emerging Technologies'*, at 253.
[423] European Parliamentary Research Service (EPRS), '*What if blockchain offered a way to reconcile privacy with transparency*?', Scientific Foresight: What if?, (2018), at 2.
[424] EU AI Act, Key Issue 5, Transparency Obligation.
[425] 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, Brussels, (2021), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

specifically and comprehensively tackling Artificial Intelligence[426], since it allows citizens to understand the design and usage of AI systems, as well as hold companies and public authorities accountable for their decisions.

The GDPR requirements on preventive measures, particularly those involving privacy by design and by default, do not limit the development of AI systems if correctly planned and implemented, even though they may incur some additional expenses. It must be established which AI applications represent high risks and so require a preventive data protection evaluation, as well as maybe the preventive engagement of data protection authorities. This makes for the EU all the more important to focus on enhancing its Data Protection framework in order to maintain its reputation of golden standard all over the world.

On the other hand, principles of data limitation purpose and minimization-related issues are the most difficult to address, given how extensively these technologies rely on data. However, there are ways to interpret, apply, and develop these data protection principles in ways that are consistent with the beneficial uses of AI and big data. The prerequisite of purpose limitation can be understood in a way that is compatible with AI and big data, through a flexible application of the concept of compatibility, which allows for the reuse of personal data when it is not incompatible with the original purposes for which the data were collected. Furthermore, reuse for statistical purposes is presumed to be compatible, and hence would be permissible in general (unless it posed unacceptable dangers to the data subject)[427].

As to data minimization, in order to overcome issues it may be necessary, in some cases, to decrease the 'personality' of available data rather than the quantity of such data, this meaning reducing the ease with which the data can be linked to persons by procedures such as pseudonymization[428]. The possibility of re-identification does not imply that all re-identifiable data should be regarded personal data and should be kept to a minimum. Re-identification of data subjects, on the other hand, should be seen as the generation of new personal data, subject to all applicable restrictions. Re-identification shall be absolutely banned unless all prerequisites for the authorized collection of personal data are met, and it

[426] European Parliament, 'EU AI Act: first regulation on artificial intelligence', European Parliament News, (2023).
[427] Supra European Parliamentary Research Service (EPRS), '*The impact of General Data Protection Regulation on Artificial Intelligence*', Scientific Foresight, (2020), at II.
[428] *Ibid.*

should be compatible with the original reasons for which the data were obtained and then anonymized.

Pseudo-anonymization serves as an important cornerstone within numerous GDPR compliance-focused solutions proposed by scholars and experts. Alongside transparency, it stands out as a pivotal element in achieving and maintaining compliance with the GDPR. Its significance has grown even more pronounced with the upcoming introduction of the EU Data Act[429], as it addresses and alleviates the complexities arising from datasets containing a blend of personal and non-personal data (addressing both)[430] and provides for the development of interoperability standards for data to be reused between sectors[431].

In waiting for the new cited legal instrument to entry into force and implement the current framework, we can already conclude that while difficulties emerge, on the other hand the GDPR offers a nuanced framework for emerging technologies that challenges them to be more than just effective or innovative. Pushing them to respect the data that fuels them, and to consider the privacy of the end-user as a critical performance metric, technologies are now gauged not just by their functionality or convenience but also by how responsibly they handle user information. While doing so, it pushes for a realm of technological development where privacy and functionality are not trade-offs but complementary objectives.

Looking ahead, the aspiration is that forthcoming legislation will facilitate a smoother transition for organizations, enhancing the EU's competitive edge and reinforcing its position as the global standard-bearer for data protection. This entails the need for new regulations to strike a delicate balance between innovation and privacy, encourage adaptability to evolving technology, and promote international data flows, while nurturing trust and transparency. By achieving this equilibrium, the EU can continue to lead the world in safeguarding data privacy while fostering technological progress.

[429] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).
[430] In detail, see Bárbara Da Rosa Lazarotto, Gianclaudio Malgieri, '*The Data Act: a (slippery) third way beyond personal/non-personal data dualism?',* European Law Blog, (2023).
[431] Council of the EU, 'Data act: Council and Parliament strike a deal on fair access to and use of data', Press Release, (2023).

CONCLUSIONS

This thesis aims at providing a comprehensive analysis of the General Data Protection Regulation and critically assess whether (and if so, to what extent) the Regulation successfully achieves its dual mandate of safeguarding the protection of data while promoting the efficient functioning of the Internal Market. To do so, we began by tracking the historical and legal path towards the Regulation, understanding the very roots from which the European Data Protection framework originated.

In retracing the main events that led to its formulation and the most influential judgements issued by the Court of Justice, each playing a pivotal role in clarifying the interpretation and application of the Regulation, the initial focus ended by providing some original keys to better appreciate some of the Regulation's nuances, addressing how the balancing of market-oriented evaluations with other instances is rooted in the lawmaking of the EU and how this emerges on nowadays policies with GDPR making no exception.

Through this prism, the thesis entered its core by researching whether the GDPR strikes a good balance in pursuing its two primary goals: the protection of personal data and ensuring the free movement of such data in the EU.

Stressing the fundamental importance of a functioning digital internal market in nowadays society, we gave our attention to the framework put forward to ensure the freedom of movement of personal and non-personal data in the EU from the Regulation, which we referred to as a - much needed - "fifth-freedom". Bearing this in mind, we proceeded to tackle GDPR's main provisions and principles for the safeguarding of data subjects' rights in order to acknowledge whether these could be hindered by some of the provisions of the same Regulation which appear to give some undue space of manoeuvre to undertakings (see automated decision-making).

What emerged from the analysis of the most sensible areas of the Regulation and, most of all, of the most recent decisions of the Court of Justice (*Meta v. Bundeskartellamt,* 2023), is a marked stance from EU institutions for which privacy rights are non-negotiable, and seemingly not even balance-able when it comes to market concerns. In addressing how, while prizeworthy, pursuing such an absolutization of what is not an absolute right can lead to consistent market-related issues, we can infer that the framework laid down for the free

movement of data does not – and presumably will not – hinder privacy concerns at the very least. *A contrario* the argument remains valid: the last chapter, in fact, showed how notwithstanding the sensation caused by the entry into force of the Regulation, implementation was not the nightmare that was anticipated. On the contrary, we have seen how several different studies showcased overtly satisfied stakeholders whereas in many cases the pursuit of compliance, initially driven by the desire to avoid the significant fines imposed by the GDPR, ultimately translated into substantial benefits for these undertakings.

In sum, the resulting framework appears to acknowledge a primacy of the protection of fundamental rights while precluding unnecessary restrictions on data flows, striking a good balance in safeguarding both EU users' rights – wherever the processing may take place – and in bolstering innovation and a dynamic market for stakeholders to exploit.

Whether as a manifestation of the "*Brussels effect*" or a simple acknowledgement of its achievements beyond the European borders, the Regulation has been used as a blueprint for the creation of data protection laws worldwide and being looked up to as the global standard in jurisdiction.

The research also focused on the flaws and grey areas left by the Regulation, such as the issues in enforcement, the cost of compliance for SMEs and the conflict of core principles of the Regulation as well as of it"technology-neutral" approach (which admittedly allows it to be a dynamic discipline that takes into account the incessant technological evolution) with emerging technologies among others. Clearly, further intervention from the European legislator is necessary to ensure the European Data Protection framework maintains its prominent role and evolves to meet the demands of a rapidly changing digital landscape.

All in all, this thesis has undertaken its examination of the General Data Protection Regulation (GDPR) delving into its multifaceted nature and the varied responses it has elicited. The GDPR is a piece of legislation tasked with the complex task even more balancing the sometimes conflicting interests of data protection and the promotion of the internal market. Like any intricate regulatory framework, it comes with its imperfections, rightfully facing both enthusiastic support and criticism.

Critics may sometimes approach the GDPR from a perspective that emphasizes one of the Regulation's aims over the other. We argue that such a narrow viewpoint can lead to an unbalanced assessment. When viewed comprehensively, the GDPR yields positive outcomes. As with any evolving regulation, there is always room for improvement and

refinement. Nonetheless, it can be considered a significant achievement in data protection law and serves as a model for similar initiatives worldwide.

BIBLIOGRAPHY

BOOKS, MONOGRAPHS, COLLECTIVE WORKS

BALDWIN R., *Understanding Regulation: Theory, Strategy, and Practice,* Oxford University Press, Oxford, 1999

BALDWIN R., CAVE M., LODGE M., *The Oxford Handbook of Regulation, Oxford University Press,* Oxford, 2010

BIEBRICHER T. *Geistig-Moralische Wende. Die Erschöpfung Des Deutschen Konservatismus*, Matthes and Seitz, Berlin, 2021

CORRALES M., FENWICK M., FORGÓ N., *New Technology, Big Data and the Law,* Kyushu University, Fukoka, 2017

DYSON K., FEATHERSTONE K., *The Road To Maastricht: Negotiating Economic and Monetary Union,* Oxford University Press, 2000

DROŻDŻ A., *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR*, European Monographs 113, Walters Kluwer, Alphen aan den Rijn, 2019

KUNER C., *The EU Geneal Data Protection Regulation: A Commentary*, Oxford Pubblication, Oxford, 2021

PEACOCK A., *Germany's Social Market Economy Origins and Evolution*, Palgrave Macmillan, London, 1989

POLLICINO O., *Judicial protection of fundamental rights on the Internet: A road towards digital constitutionalism?,* Hart Publishing, Oxford, 2021

RUSSEL S. AND NORVIG P. (EDS), *Artificial Intelligence: A Modern Approach, Prentice Hall Series* In Artificial Intelligence, 2003

SCHMIDT V., THATCHER M., *Resilient Liberalism in Europe's Political Economy*, Cambridge University Press, Cambridge, 2013

TALANI S. L., ROBERTO R., '*The Dark Side of Globalisation'*, Palgrave Macmillan, London, 2019

THOMSON C.J., *Under Constant Supervision*, BookRefine Publishing, 2020

VAN DER SLOOT B., BROEDERS D., SCHRIJVERS E. (eds.), *Exploring the Boundaries of Big Data*, The Netherlands, Amsterdam, 2016

VERMEULEN G., LIEVENS E. (eds)., *Transatlantic tensions, EU surveillance, and big data,* Maklu, Antwerp, 2017

VOSS G., WOODCOCK K., *Navigating EU privacy and data protection laws,* ABA Section of International Law, Washington 2016

WATSON A., *Legal Transplants: An Approach to Comparative Literature (2nd edition)*, University of Georgia School of Law, Athens 1993

ARTICLES AND ESSAYS

ALEXOPOULOS AND OTHERS, *Benefits and Obstacles of Blockchain Applications in e-Government*, in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, January 2019, pp. 3377-3386

BERRY S., GAYNOR M., MORTON F.S. *Do increasing markups matter? Lessons from empirical industrial organization* in Journal of Economic Perspective Vol.33 No.3, Summer 2019, pp. 44-68

BENTZEN H. and HØSTMÆLINGEN N. *Balancing Protection and Free Movement of Personal Data: The New European Union General Data Protection Regulation'*, Annals of Internal Medicine Vol. 170 No. 5, February 2019, pp. 335-338

BORGESIUS F., *The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression*, in *Theoretical Inquiries in Law*, Forthcoming Vol. 19, April 2018, pp. 291-322

BOVENS M., *Analysing and Assessing Accountability: A Conceptual Framework*, in *European Law Journal* Vol. 13 No.4, July 2007, pp. 447-468

BRADFORD A., *The Brussels Effect: How the European Union Rules the World*, in *Oxford University Press*, December 2019

BREITBARTH P., *The impact of GDPR one year on*, in *Network Security*, July 2019, pp. 11-13

BRINNEN M. AND WESTMAN D., *What's wrong with the GDPR?*, in *Svenskt Näringsliv*, December 2019, pp. 1-36

BRUNO F., *Ordoliberal ideas on Europe: two paradigms of European economic integration*, in *History of European Ideas* Vol. 49, Nov 2022, pp. 737-756

BUCKLEY G., CAULFIELD T. AND BECKER I., *"It may be a pain in the backside but..." Insights into the resilience of business after GDPR*, in *Proceedings of the 2022 New Security Paradigms Workshop*, October 2022

BURRY M. AND SCHÄR R., *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, in *Journal of Information Policy* Vol. 6, June 2016, pp. 479-511

BUTTERWORTH M., *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law & Security Review* Vol. 34, February 2018

CADWALLADR C. AND GRAHAM-HARRISON E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, in *The Cambridge Analytica Files*, March 2018

CANAAN R., The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law, Centre for Law, Technology and Society, University of Ottawa Vol. 12, February 2023

CASTETS-RENARD C., *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making* in Fordham Intellectual Property, Media & Entertainment Law Journal, Forthcoming, Vol. 30 No.1, June 2019, pp. 91-137

CIRIAN S., *The Economic Impact of the European Reform of Data Protection*, in *Communications & Strategies* No. 97, October 2015, pp. 41-58

COCHRANE L., JASMONTAITE-ZANIEWICZ L. AND DAVID BARNARD-WILLS, *'Data Protection Authorities and Their Awareness-Raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-Size Enterprises',* in European Data Protection Law Review Vol. 6 Issue 3, March 2020, pp. 352-364

COMANDÈ G., SCHNEIDER G., *Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities*, in *Computer Law & Security Review* Vol.41, July 2021, pp. 1-5

CONGIU R., SABATINO L. AND SAPI G., *The Impact of Privacy Regulation on Web Traffic: Evidence From the GDPR,* in *Information Economics and Policy*, February 2022, pp. 1-43

COSTA-CABRAL F., and LYNSKEY O., *Family ties: the intersection between data protection and competition in EU Law*, in *Common Market Law Review*, Vol. 54 Issue 1, February 2017, pp. 1-31

CUSTERS B., MALGIERI G*., Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, in *Computer Law & Security Review* Volume 45, July 2022, pp.1-11

DE HERT P. AND GUILLERMO LAZCOZ, '*When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance*', European Data Protection Law Review Vol. 8 No.1, January 2022, pp. 31-40.

DECKELBOIM S.J., '*Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU–US Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses,* in *Georgetown Journal of International Law* Vol.48 No.1, Fall 2016 pp.263-296

DETERMANN L., *Healthy Data Protection*, in *Michigan Telecommunication & Technology Law Review* Vol. 26 Article 3, January 2020, pp. 229-278

DE TERWANGNE C., *A modernised international treaty for the protection of personal data*, in *Computer Law & Security Review* Vol. 40, April 2021

DOMINGO-FERRER J., *Personal big data, GDPR and anonymization*, in *Flexible Query Answering System Cham*, September, 2019, pp. 7–10.

DWORKIN G., *The Younger Committee Report on Privacy*, in *The Modern Law Review* Vol.36, No. 4, July 1973, pp. 399-406

EDWARDS L., *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, in *European Data Protection Law Review*, January 2016, pp. 1-37

EL-GAZZAR R AND STENDAL K., *Examining How GDPR Challenges Emerging Technologies*, in *Journal of Information Policy*, November 2020, pp. 237-275

EUCKEN W., *What Kind of Economic and Social System?,* in *Peacock, A., Willgerodt, H. (eds) Germany's Social Market Economy: Origins and Evolution,* August 1989, pp. 27-45

FAIFR A. AND JANUSKA M., *Companies´ readiness of GDPR and implementation barriers*, in *41st International Academic Conference, Venice*, September 2018, pp. 31-47

FAN W., GEERTS F., WIJSEN J., *Determining the Currency of Data*, in *ACM Transactions on Database Systems*, Vol. 37, No. 4, December 2012, pp. 1-46

FERRAND B., *The Ordoliberal Internet? Continuity and Change in the EU's approach to the Governance of Cyberspace*, in *Cambridge University Press* Vol. 2, June 2023, pp. 106-126

FOUSKAS V., *Placing Austerity in Context: The Greek Case Between Neo-Liberal Globalisation and an Ordoliberal EU*, in *Talani, Leila Simona and Roccu, Roberto, The Dark Side of Globalisation*, March 2019

FRANTZIOU E., *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12,* in *Human Rights Law Review* Vol. 14, October 2014, pp. 761-777

FREITAS M. AND DA SILVA M., *GDPR Compliance in SMEs: There is much to be done*, in *the Journal of Information Systems Engineering & Management* Vol.34 No.4, November 2018, pp. 1-7

GALLAGHER B., *Will the U.S. Adopt a Nationwide Data Privacy Law Similar to GDPR?*, in *Partners*, August 2022

GARBER J., *GDPR – compliance nightmare or business opportunity?*, in *Computer Fraud & Security* Vol. 2018, June 2018, pp. 14-15

GARDINER P. AND ABBOTTS G., *Scarlet extended reprieve from content filtering*, in *Entertainment Law Review*, February 2012

GERNIT H., *A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012*, in *A Journal of Law*, May 2012

GILMAN M., Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice, in Arizona State Law Journal Vol. 52, August 2020, pp.368-444

GLOBOCNIK J., *On Joint Controllership for Social Plugins and Other Third-Party Content – A Case Note on the CJEU Decision in Fashion ID*, in *International Review of Intellectual Property and Competition Law 2019/50*, No. 8, September 2019 pp. 1033-1044

GODDARD M., *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, in *International Journal of Market Research* Vol. 58, November 2017, pp. 703-705

GODYN M. AND OTHERS, *Analysis of solutions for a blockchain compliance with GDPR*, in *Scientific Reports*, September 2022, pp. 1-11

GONZALEZ E.G. AND DE HERT P., '*Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles'*, Journal ERA Forum Vol. 2019 No. 4, February 2019 pp. 597-621

GREENGARD S., *Weighing the impact of GDPR*, in *ACM Digital Library* Vol. 61, November 2018, pp. 16-18

GUBBI J., BUYYA R., MARUSIC S. AND PALANISWAMI M., *Internet of Things (IoT): A vision, architectural elements, and future directions*, in *Future Generation Computer Systems* Vol. 29, February 2013, pp. 1645-1660

GUNST S. AND DE VILLE F., *The Brussels Effect: How the GDPR Conquered Silicon Valley*, in *European Foreign Affairs Review* Vol. 26, November 2021, pp. 437-458

HADDARA M., SALAZAR A. AND LANGSETH M., *Exploring the Impact of GDPR on Big Data Analytics Operations in the E-Commerce Industry*, in *E-Commerce Industry, Procedia Computer Science* Vol. 219, March 2023, pp. 767-777

HAWATH M., *Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR'*, in *European Data Protection Law Review* Vol. 7 Issue 2 pp. 161-173

HERIAN R., *Regulating Disruption: Blockchain, Gdpr, and Questions of Data Sovereignty*, in *Journal of Internet Law* Vol. 22, June 2020, pp. 1-16

HIEN J., *European integration and the reconstitution of socio-economic ideologies: Protestant ordoliberalism vs social Catholicism*, in *Journal of European Public Policy* Vol. 27, May 2020, pp. 1368-1387

HIEN J., *The rise and fall of ordoliberalism*, in *Socio-Economic Review* Vol. 00, No. 0, April 2023, pp. 1-20

HIIMANS H. AND SCIROCCO A., *Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?*, in *Common Market Law Review* Vol.46 No.5, October 2009, pp. 1485-1525

HILDEBRANDT M., *Slaves to Big Data. Or Are We?*, in *idp. revista de internet, derecho y politica*, October 2013, pp. 27-44

HOFHEINZ P., MICHAEL M., *Uncovering the Hidden Value of Digital Trade,* Interactive Policy Brief, in Interactive Policy Brief Vol. 19, July 2015, pp. 1-12

HOFFMAN D., BRUENING S. AND CARTER S., *The Right to Obscurity: How We Can Implement the Google Spain Decision*, in *North Carolina Journal of law & technology* Vol. 17, March 2016, pp. 437-482

HOOFNAGLE C.J., VAN DER SLOOT B., AND BORGESIUS F.*, The European Union general data protection regulation: what it is and what it means*, in *Information & Communications Technology Law* Vol. 28 No.1, February 2019, pp. 65 - 98

IRWIN L., *Organisations struggling to meet GDPR requirements, with poor planning and lack of awareness to blame*, in *IT Governance Blog*, June 2019

JOHNSON G., SHRIVER S., GOLDBERG S., *Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR,* in *Management Science* Vol.0:Ahead of Print, March 2022 pp.1-27

KIRSTEN M., *Privacy notices as tabula rasa: an empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online,* in Journal Public Policy Mark. Vol. 34 No.2, September 2015, pp. 143-303

KOOPS B., *Should ICT Regulation Be Technology-Neutral?*, in *IT & Law Series* Vol.9, July 2006, pp. 77-108

KORPELA K., HALLIKAS J. AND DAHLBERG T., *Digital Supply Chain Transformation toward Blockchain Integration*, in *Proceedings of the 50th Hawaii International Conference on System Sciences* Vol.50, January 2017, pp. 4182-4191

KSHETRI N., *Privacy and security issues in cloud computing: The role of institutions and institutional evolution*, in *Telecommunications Policy* Vol.37, July 2012, pp. 372-386

KULK S. AND BORGESIUS F., *Google Spain v. González: Did the Court Forget about Freedom of Expression?*, in *Cambridge University Press* Vol. 5, N. 3, pp. 389-398

KUNER C., *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal* Vol. 18 No. 4, March 2016, pp. 882-918

LAYTON R. AND MCLENDON J., *The GDPR: What It Really Does and How the U.S. Can Chart a Better Course*, in *Federalist Society Review* Vol. 19, October 2018, pp. 234-248

LAYTON R. and ELALUF-CALDERWOOD S., *A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices*, 12th CMI Conference on Cybersecurity and Privacy (CMI), November 2019, pp. 1-6,

LANGFORD M., *Taming the Digital Leviathan: Automated Decision-Making and International Human Rights, American Journal of International Law - Unbound,* Vol. 114, pp. 141-146, June 2020

LI H., YU L., HE W., *The Impact of GDPR on Global Technology Development*, in *Journal of Global Information Technology Management* Vol.22, January 2019, pp. 1-6

LINDMAN J., ROSSI M. AND TUUNAINEN V., *Opportunities and risks of Blockchain Technologies in payments– a research agenda*, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, January 2017, pp. 1533-1542

LINSKEY O. AND GENTILE G., '*Deficient by design? The transnational enforcement of the GDPR'* in *International and Comparative Law Quarterly*, Vol.71, pp-799-830

LUISI M., *GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion*, in *E-International Relations*, April 2022

LUTZ F., *Observations on the Problem of Monopolies*, in *Alan Peacock and Hans Willgerodt (eds), Germany's Social Market Economy: Origins and Evolution (Palgrave Macmillan UK 1989)*, August 1989, pp. 152-170

MAHIEU R., VAN HOBOKEN J. AND ASGHARI H., *Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe*, in *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, May 2019, pp. 39-59

MAHER I., *Re-Imagining the Story of European Competition Law*, in *Oxford University Press* Vol. 20 No. 1, Spring 2000,pp. 155-166

MAKHDOM I., ABOLHASAN M., ABBAS H. AND NI W., *Blockchain's adoption in IoT: The challenges, and a way forward*, in *Journal of Network and Computer Applications*, January 2019, pp. 251-279

MALDOFF G., TENE O. *'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example,* in Wisconsin International Law Journal, Forthcoming, January 2017, pp. 1-65

MARKOPOULOUA D., PAPAKONSTANTINOUA V., DE HERT P., *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation,* in *Computer law & security review* Vol.35, Issue 6, November 2019

MCALLISTER C., *What about Small Businesses: The GDPR and Its Consequences for Small, U.S.-Based Companies,* in *Brooklyn Journal of Corporate, Financial & Commercial Law* Vol. 12, December 2017, pp. 187-211

MCQUINN A. AND CASTRO D., *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, in *Information Technology and Innovation Foundation*, August 2019

MITROU L., *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, in *Tilburg: TILT Law & Technology*, January 2018, pp. 1-90

MOHAN J., WASSERMAN M. AND CHIDAMBARAM V., *Analyzing GDPR Compliance Through the Lens of Privacy Policy*, in *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, October 2019, pp. 82-95

MONROE B., *The Five Vs of Big Data Political Science Introduction to the Virtual Issue on Big Data in Political Science Political Analysis*, in *Cambridge University Press* Vol. 21, January 2017

MOSS B., *The European Community as Monetarist Construction: A Critique of Moravcsik*, in *Journal of European Area Studies* Vol. 8, August 2010, pp. 247-265

NEDERGAARD P., *The Influence of Ordoliberalism in European Integration Processes - A Framework for Ideational Influence with Competition Policy*

and the Economic and Monetary Policy as Examples, in *MPRA Paper*, December 2013, pp. 1-32

NINO M., *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale* Vol. 14 Fascicolo 3, December 2020, pp. 733-759

O'SULLIVAN K., *Enforcing Copyright Online: Internet Service Provider Obligations and the European Charter of Fundamental Rights*, in *European Intellectual Property Review*, September 2014, pp. 1-12

PAUN M., *On the Way to Effective and Complete Protection (?): Some Remarks on Fashion ID*, in *Journal of European Consumer and Market Law* Vol.9, January 2020, pp. 35-36

PELOQUIN D., DI MAIO M., BIERER B, BARNES M., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data,* in *European Journal of Human Genetics* Vol. 28, March 2020, pp. 697-705

POLINSKY M., SHAVELL S., *The economic theory of public enforcement of law* in *Journal of Economic* Vol. 38 No.1, March 2000, pp.45-76

POLITOU E., ALEPIS E. AND PATSAKIS C., *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, in *Journal of Cybersecurity* Vol. 4, March 2018, pp. 1-20

PSYCHOGIOPOULOU E., *Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers after Scarlet / E. Psychogiopoulou*, in *European Intellectual Property Review* Vol. 34, No. 8, July 2012, pp. 552-554

RESTA G., '*La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE'*, in *Il diritto dell'informazione e dell'informatica*, Vol. 31, No. 4-5, 2015, pp. 697-718

RICHARDS N. AND HARTZOG W., '*Taking Trust Seriously in Privacy Law'*, in *Stanford Technology Law Review* 19, September 2016, pp. 431-472

RICHARDS N. AND HARTZOG W., *The Pathologies of Digital Consent*, in *Washington University Law Review* Vol. 96, April 2019, pp. 1461-1503

ROSENBERG M., CONFESSORE N. AND CADWALLADR C., *How Trump Consultants Exploited the Facebook Data of Millions*, in *The New York Times*, March 2018

ROTHKEGEL T. AND STRASSEMEYER L., *Joint Control in European Data Protection Law – How to make Sense of the CJEU's Holy Trinity - A case study on the recent CJEU rulings (Facebook Fanpages; Jehovah's Witnesses; Fashion ID)*, in *Computer Law Review International*, December 2018

ROUVROY A., *"of data and men" : fundamental rights and freedoms in a world of big data*, in *Academia*, January 2016, pp. 1-37

RYNGAERT. C. AND TAYLOR M., *The GDPR as global Data Protection Regulation?*, in *Symposium on the GDPR and International Law* Vol.114, January 2020, pp. 5-9

SCHARPF F.W., *Towards a more democratic Europe: De-constitutionalization and Majority Rule*, in *Zeitschrift Für Staats- Und Europawissenschaften*, Vol. 23, January 2017, pp. 84-118

SCHWARTZ P., *Global Data Privacy: The EU Way*, in *New York University Law Review* Vol. 94, October 2019, pp. 783-817

SCOTT J., *Extraterritoriality and Territorial Extension in EU Law*, in *American Journal of Comparative Law*, Vol. 62, No. 1, December 2013, pp. 87-125

SHARMA O., *How Does GDPR Impact Emerging Technologies?*, in *Data and Technology Insights*, July 2022

SIRUR S., NURSE J. AND WENN H., *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*, in *ArXyv*, August 2018, pp. 1-8

STREECK W., *Heller, Schmitt and the Euro*, in *European Law Journal* Vol. 21, No. 3, May 2015, pp. 361-370

SOMBRA T., *The General Data Protection Law in Brazil: What Comes Next?*, in *Global Privacy Law Review* Vol. 1, June 2020, pp. 78-80

SUBRAMANIAN A., *GDPR Cost and Implementation Concerns for Businesses*, in *Medium*, June 2019

TEIXEIRA G., DA SILVA M., DE SOUSA R., *The critical success factors of GDPR implementation: a systematic literature review*, in *Digital Policy Regulation and Governance* Vol. 21 No.4, June 2019

THATCHER M. AND A. SCHMIDT V., *Supranational neo-liberalization: The EU's regulatory model of economic markets*, in *Cambridge University Press*, June 2014

TIKKINEN C. AND ROHUNEN A., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in *Computer Law & Security Review* Vol. 34, February 2018, pp. 134-153

UNDERWOOD S., *Blockchain beyond bitcoin*, in *Communications of the ACM* Vol. 59, November 2016, pp. 15-17

URQUHART L., LODGE T. AND CRABTREE A., *Demonstrably doing accountability in the Internet of Things*, in *International Journal of Law and Information Technology* Vol. 27, December 2018, pp. 1-27

UTZ C., DEGELING M., FAHL S., SCHAUB F., AND HOLZ T. *(Un)informed Consent: Studying GDPR Consent Notices in the Field,* in ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 2019, pp. 1-18

VAN DER SLOOT B. AND VAN SCHENDEL S., *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, in *Jipitec*, March 2017

VIDOVIĆ S., *Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities*, in Croatian Yearbook of European Law and Policy Vol. 11 No.1, October 2015, pp. 259-276

VLAHOU A. ET AL., *Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics*?, in Hypertension vol. 77, February 2021, pp. 1029-1035

VOSS G., *Cross-Border Data Flows, the GDPR, and Data Governance*, in *Washington International Law Journal* Vol. 29 No. 3, January 2020, pp. 484-532

YEOUNG K., BYGRAVE L., '*Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*', *in Regulation & Governance*, Vol. 16, Issue 1, Januray 2022, pp. 1-354

YOUNG B., *German Ordoliberalism as Agenda Setter for the Euro Crisis: Myth Trumps Reality*, in *Journal of Contemporary European Studies* Vol. 22, August 2014, pp. 276-287

YUEH J., *GDPR Will Make Big Tech Even Bigger,* in *Forbes Technology Council*, June 2018

WARLOUZET L., *Governing Europe in a Globalizing World*, in *London: Journal of Common Market Studies* Vol. 57, No. 1, June 2018, pp. 77-93

WARLOUZET L., *The EEC/EU as an Evolving Compromise between French Dirigism and German Ordoliberalism (1957–1995)*, in *JCMS: Journal of Common Market Studies* Vol. 57, January 2019, pp. 77-93

WARREN T., *Explaining the European Central Bank's limited reform ambition: ordoliberalism and asymmetric integration in the eurozone*, in *Journal of European Integration* Vol. 42, September 2019, pp. 263-279

WATCHER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* in *International Data Privacy Law* Vol. 7, No. 2, January 2017, pp. 76-99

WATCHER S., *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*, in *Computer Law & Security Review*, December 2017, pp. 1-22

WATCHER S., *The GDPR and the Internet of Things: A Three-Step Transparency Model, in Law*, in *Innovation and Technology*, March 2018, pp. 1-32

WEBBER M., *The GDPR's impact on the cloud service provider as a processor*, in *Privacy & Data Protection* Vol. 16, March 2016

ZALNIERIUTE M. AND CHURCHES G., *When a 'Like' Is not a 'Like': A New Fragmented Approach to Data Controllership*, in *The Modern Law Review (Forthcoming)*, January 2019, pp. 1-26

ZARSKY T., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review* Vol. 47, August 2017, pp. 995-1020

ZHOU C., BARATI M., AND SHAFIQ O., *A compliance-based architecture for supporting GDPR accountability in cloud computing*, in *Future Generation Computer Systems* Vol. 145, August 2023, pp. 104-120

OTHER ARTICLES AND STUDIES

BIEGA A., POTASH P., DAUMÉ H., DIAZ F. AND FINCK M., *Operationalizing the Legal Principle of Data Minimization for Personalization,* in *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development,* May 2020.

BIRD & BIRD, '*Big Data issues & Opportunities, Free flow of Data'*, Bird&Bird Insights, 18 February 2019

BERNSTEIN C., *Personally Identifiable Information (PII*)', TechTarget, February 2023

BOLOGA A., *Fifty Shades of GDPR Privacy: The Good, the Bad, and the Enforcement*, CEPA, 7 February 2023

BURGESS M., *How GDPR is failing,* Wired UK Security, 23 May 2022

BUTTARELLI G., *8th Annual Data Protection and Privacy Conference*, 30 November 2017

CASTRO D., *The False Promise of Data Nationalism,* The Information Technology & Innovation Foundation, 9 December 2013

CHLIPALA M. AND PILAR S., *CLOUD SERVICE PROVIDER – PROCESSOR, CONTROLLER OR BOTH?*, in *International Network of Privacy Law Professionals*, 31 August 2017

CHRISTIAKIS T., *After Schrems II*, European Law Blog, 21 July 2020

CLEARWATER A, AND PHILBROOK B., *GDPR Enforcement: Is it really about the fines?*, in *The International Association of Privacy Professionals*, June 2018

COMFORTE, *Three Key Risks and Opportunities of GDPR*, Comforte AG, 2018

Commission Nationale de l'Informatique et des Libertés (CNIL), France, European Data Protection Supervisor (EDPS), European Union, Garante per la protezione dei dati personali, Italy, 40th International Conference of Data Protection and Privacy Commissioners, in Declaration ethics and data protection in artificial intelligence, October 2018, Brussels

COMMISSION OF THE EUROPEAN COMMUNITIES, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century*, White Paper of the EU Commission, December 1993

COMMISSION OF THE EUROPEAN COMMUNITIES, Staff working document impact assessment *accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union,* September 2017

COMMISSION OF THE EUROPEAN COMMUNITIES, *'Annex to the Synopsis Report. Detailed Analysis of the Public Online Consultation Results on 'Building a European Data Economy*', Setpember 2017

DAVIES H., *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, The Guardian, 11 December 2015

DESJARDINS G., *Your Personal data is the currency of the digital age*, La Conversation, 24 September 2020

DONN P., *GDPR 5 years on*, in Data Protection Network, May 2023

DUARTE D., *An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR,* in *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law*, 24 March 2020, pp. 1-58

DULLIEN S. AND GUÉROT U., *The long shadow of ordoliberalism: Germany's approach to the euro crisis*, in *European Council of Foreign Relations*, 22 February 2012

EISS R.,*Confusion over Data-privacy Law Stalls Scientific Progress*, Nature, 25 August 2020

EUROPEAN PARLIAMENTARY RESEARCH SERVICE (EPRS), *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?*, Panel for the Future of Science and Technology, July 2019

EUROPEAN PARLIAMENTARY RESEARCH SERVICE (EPRS), *What if blockchain offered a way to reconcile privacy with transparency?*, Scientific Foresight: What if?, 27 September 2018

Executive Office of the President National Science and Technology Council National Science and Technology Council Committee on Technology, *Preparing for the Future of Artificial Intelligence*, October 2016

FASANO G., *Dati personali: da «res extra commercium» a moneta di scambio*, Il Sole 24Ore, 4 January 2022

FERRACANE M., *Restrictions on Cross-Border Data Flows: A Taxonomy*, ECIPE Working Paper, December 2017

FINLAY A. AND MADIGAN R., *GDPR and the Internet of Things: 5 Things You Need to Know*, in *McCann FitzGerald LLP*, May 2016

GAO L., ELLEN K. AND EGGERS A., *GDPR and the cloud: examining readability deficiencies in cloud computing providers' privacy policies*, in *Policy Studies,* 2 October 2022

GOOD O.W., *Super Monday Night Combat will close down, citing EU's new digital privacy law,* Polygon, 28 April 2018

GUTTA S., *Data Science: The 5 V's of Big Data*, in *Medium*, 4 May 2020

HAQUE B. AND OTHERS, *GDPR Compliant Blockchains-A Systematic Literature Review*, in *Cornell University*, 1 April 2021

HERCHER J., *Drawbridge Exits Media Business In Europe Before GDPR Storms The Castle*, AD exchanger 7 March 2018

HOFHEINZ P. and OSIMO D*., Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age,* The Lisbon Council Policy Brief: Making Europe a Data Economy, 25 July 2017

HUDDLESTON J., *Takeaways from the GDPR, 5 Years Later*, in *CATO Institute*, May 2023

HUNTON ANDREWS KURTH LLP, *CJEU Applies Broad Territorial Scope to EU Data Protection Law,* 5 October 2015

IRWIN L., *GDPR: Understanding the 6 data protection principles*, IT Governance European Blog, 9 December 2021

JONES A., *GDPR Three Years Later: What Impact Has It Made?*, in *Partners*, August 2022

HAQUE B. AND OTHERS, *GDPR Compliant Blockchains-A Systematic Literature Review*, in *Cornell University*, 1 April 2021

HAUPTFLEISCH W., *GDPR — Establishing A Fundamental Right, Not Just Regulation,* Medium, 6 October 2022

KALA K., *Free movement of data as the 5th fundamental freedom of the European Union*, e-Estonia, 6 October 2017.

KELLEHER D., *You're Watching Schrems, but Maybe You Should Be Watching Weltimmo,* IAPP, 26 May 2015

KOTTASOVÁ I., *These companies are getting killed by GDPR*, in *CNN Business*, May 2018

KUCHLER H., *US small businesses drop EU customers over new data rule*, in *Financial Times*, 24 May 2018

KUNER C., *The Schrems II Judgment of the Court of Justice,* European Law Blog, 17 July 2020

KÜSTERS A., *The Making and Unmaking of Ordoliberal Language. A Digital Conceptual History of European Competition Law (c.1950-2020)*, in *University of Frankfurt*, Doctoral thesis, June 2022

LARRÚ I., *The Rising Value of Data*, IE Insights, 11 April 2018

LAYTON R. AND ELAUF-CALDERWOOD S., *A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices*, in *12th CMI Conference on Cybersecurity and Privacy*, November 2019

LAZZAROTTO B. AND MALGIERI G., *The Data Act: a (slippery) third way beyond personal/non-personal data dualism?*, in *European Law Blog*, May 2023

LIWER D., *GDPR: one size does not fit all*, CSO online, 1 May 2018

LOTTERING L., *Balancing Privacy and Digital Marketing in the Information Age*, CM Blog, 11 November 2021

MASSIMINI M., *Effetto GDPR depotenziato tra debolezze di enforcement e "braccino" irlandese*, Privacy.it 4 October 2021

MCKINSEY GLOBAL INSTITUTE, *Digital globalization: The new era of global flows,* Report, 24 February 2016

MCKINSEY GLOBAL INSTITUTE, *Globalization in transition: The future of trade and value chains,* Report, 16 January 2019

MUNCASTER P., *Firms Already Swamped by Right to be Forgotten Requests*, in *Infosecurity Magazine*, 12 January 2016

NEMITZ P., *Constitutional democracy and technology in the age of artificial intelligence*, in *Royal Society Philosophical Transactions*, 15 October 2018

SHARMA O., *How Does GDPR Impact Emerging Technologies?*, in *Data and Technology Insights*, July 2022

OXFORD ANALYTICA*, GDPR enforcement will improve slowly in the EU,* Expert Briefings, 21 November 2022

PAGALLO U. AND OTHERS, AI4People - *On Good AI Governance: 14 Priority Actions, a S.M.A.R.T. Model of Governance, and a Regulatory Toolbox*, Working Paper, November 2019

PALMER M., CLIVE H., *Data is the New Oil*, ANA Marketing Maestros*,* 3 November 2006

POLLICINO O. DUNN P., *The Sustainability of European Privacy and Data Protection,* MediaLaws, Law and Policy of the Media in a Comparative Perspective*,* 3 October 2022

RABESANDRATANA T., *'European Data Law is Impeding Studies on Diabetes and Alzheimer's*, *Researchers Warn*, Science.org, 20 November 2019

RAGAN S. AND PIRVAN P., *What is "Convention 108"?*, Wrangu, June 2018.

ROSNER L., *GDPR: Bridging The Gap Between Consumer And Marketer Perceptions*, in *Forbes Communications Council*, 10 March 2020

SATARIANO A*., G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, The New York Times, 24 May 2018

SEO J. AND OTHERS, *An analysis of economic impact on IoT under GDPR*, *8th International Conference on ICT Convergence* (ICTC), 5 December 2018

SHAH A., BANAKAR V., SHASTRI S., WASSERMAN M., CHIDAMBARAM V., *Analyzing the Impact of GDPR on Storage Systems,* 11th Usenix Workshop, 16 MAY 2019

SIMELL B. AND OTHERS, *Transnational access to large prospective cohorts in Europe: Current trends and unmet needs*. N Biotechnol, 25 March 2019

SCOTT M. AND CERULUS L., *Europe's new data protection rules export privacy standards worldwide*, in *Politico*, January 2018

UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, in Artificial intelligence: opportunities and implications for the future of decision making, 21 November 2016

WIEBE A., DIETRICH N., '*Open Data Protection, Study on Legal Barriers to Open Data Sharing- Data Protection and PSI,* Universitätsverlag Göttingen, 2017

OFFICIAL ACTS AND LEGISLATION

EU OFFICIAL ACTS AND LEGISLATION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27April 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), OJ L 119, 4.5.2016

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018

Directive (EU) 95/46/EC of the European Parliament and of the Council of European Union *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281/31, 24.10.1995

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); OJ L 333, 27.12.2022

European Commission, 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, 2021/0106(COD), 21.4.2021

European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data, 2022/0047(COD), 23.2.2022

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce, Communication from the Commission, Brussels, 16.04.1997

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Functioning of the

Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, Brussels, 27.11.2013

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building a European Data Economy, Brussels, 10.1.2017

Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A European strategy for data, Brussels 19.2.2017

OPINIONS OF AG

Opinion of Advocate General Henrik Saugmandsgaard Øe delivered on 19 December 2019., Case C-311/18, ECLI:EU:C:2019:1145.

Opinion of AG Rantos delivered on 20 September 2022., Case C-252/21, ECLI:EU:C:2022:704

INTERNATIONAL CONVENTIONS AND OFFICIAL ACTS OF INTERNATIONAL ORGANIZATIONS

COUNCIL OF EUROPE, Resolution (73)22, *The protection of the privacy of individuals vis-a-vis electronic data banks in the private sector,* adopted by the Committee of Ministers on 25 September 1973.

COUNCIL OF EUROPE, Convention 108, *the Protection of Individuals with regard to Automatic Processing of Personal Data*, adopted by the Committee of Ministers on 28 January 1981.

COUNCIL OF EUROPE, Resolution 2171 (2017), *Parliamentary scrutiny over corruption: parliamentary cooperation with the investigative media,* adopted by the Parliamentary Assembly on 27 June 2017

EUROPEAN UNION COURT OF JUSTICE CASE LAW

CJEU, Case 176/03, Commission v. Council, *Environmental crimes,* ECLI:EU:C:2005:542

CJEU, Case 553/07, College Van Burgemeester en wethouders van Rotterdam v M. E. Rijkeboer, ECLI:EU:C:2008:773

CJEU, Case 553/07, College Van Burgemeester en wethouders van Rotterdam v M. E. Rijkeboer, ECLI:EU:C:2008:773

CJEU, Case 70/10, Scarlet Extended SA v Société belge des auteurs, ECLI:EU:C:2011:771

CJEU, Case 360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, ECLI:EU:C:2012:85

CJEU, Case131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317

CJEU, Case 141/12 and Case 372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081

CJEU, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238

CJEU, Case 314/12, UPC Telekabel Wien GmbH contro Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH, ECLI:EU:C:2014:192

Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*,; ECLI:EU:C:2015:639

CJEU, Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI identifier: ECLI:EU:C:2015:650

CJEU, Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779

CJEU, Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, ECLI:EU:C:2016:970

CJEU, Case 210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388

CJEU, Case 434/16, Nowak v Data Protection Commission, ECLI:EU:C:2017:994

CJEU, Case 25/17, Tietosuojavaltuutettu v Jehovan todistajat, ECLI:EU:C:2018:551

CJEU Case 40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629

CJEU Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt*, ECLI:EU:C:2023:537.

EUROPEAN COURT OF HUMAN RIGHTS CASE LAW

ECHR, *Engel and others v. The Netherlands,* Judgment 8 June 1976

ECHR, *Axel Springer AG v. Germany*, Judgment 7 February 2012

ECHR, *Von Hannover v. Germany*, judgment 7 February 2012

SITOGRAPHY

NIST National Institute of Standards and Technology, *Definition of cloud* computing, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

PbD The '7 Foundational Principles', https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Press relase on the 11 October 2016 ECOFIN conclusions, https://www.consilium.europa.eu/it/press/press-releases/2016/10/11/ecofin-conclusions-tax-transparency/?j=1877099

Number of IoT Devices (2023), https://explodingtopics.com/blog/number-of-iot-devices#

WatchGuard Technologies, Survey Showing Confusion Around GDPR Compliance, https://securitybuyer.com/survey-shows-global-organisations-unsure-gdpr/ .

IAB internet advertising revenue report, 2017 https://www.iab.com/wp-content/uploads/2017/12/IAB-Internet-Ad-Revenue-Report-Half-Year-2017-REPORT.pdf

IAB internet advertising revenue report, 2022 https://www.iab.com/wp-content/uploads/2023/04/IAB_PwC_Internet_Advertising_Revenue_Report_2022.pdf

TikTok Newsroom https://newsroom.tiktok.com/en-eu/changes-personalised-ads-eu

GPDP, motore di ricerca provvedimenti, https://www.garanteprivacy.it/home/ricerca/-/search/tipologia/Provvedimenti

PriceWaterhouseCoopers Privacy Acts Reviews Reports, https://www.pwc.com.au/cyber-security-digital-trust.html

McKinsey Privacy Featured Insights, https://www.mckinsey.com/featured-insights

CMS Law, Tax & Future GDPR enforcement tracker https://www.enforcementtracker.com