Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

THE RIGHT TO INFORMATIONAL SELF-DETERMINATION BETWEEN LEGISLATION AND IMPLEMENTATION

Najlaa Flayyih*, Mohammed Hasson Ali, Ahmad Fadli and Khaled Aljasmi

ABSTRACT

Background*: The right to informational self-determination has emerged as a pivotal component of digital rights in the era of artificial intelligence and big data. Rooted in the broader right to privacy, this right enables individuals to control the collection, use, and dissemination of their personal data. Despite its recognition in instruments such as the General Data Protection Regulation (GDPR), a significant gap persists between the legal framework and practical implementation. The rationale of this study lies in analysing the disjunction between legislative guarantees and the realities of enforcement, with a focus on the European legal landscape. The increasing complexity of digital technologies and the emergence of new data categories—such as mental data—have challenged both legal doctrines and institutional capabilities.*

Methods*: The study employs a doctrinal legal analysis, drawing on a comprehensive examination of the GDPR provisions, judicial precedents from the Court of Justice of the European Union, national supervisory authority reports, and academic commentaries. Comparative elements are included to contextualise the European framework within broader international developments. Practical cases and regulatory enforcement patterns are used to identify gaps and assess the effectiveness of current mechanisms. The research also incorporates an analytical evaluation of algorithmic environments and their implications for consent, transparency, and individual agency.*

Results and Conclusions: *The study finds that while the GDPR offers a robust structure for personal data protection, its practical application is hindered by structural, technical, and interpretive challenges. Consent is often rendered ineffective in AI-driven contexts; individuals struggle to exercise their rights, and regulatory enforcement remains uneven across Member States. The research highlights the need for a harmonised institutional model, enhanced user interfaces, and the legal recognition of emerging data types like mental data. It concludes that bridging the legislative-implementation divide requires integrating legal, technological, and ethical tools within a cohesive framework—reaffirming the right to informational self-determination as a cornerstone of digital human dignity.*

1 INTRODUCTION

In recent decades, the digital world has witnessed a radical transformation in the relationship between individuals and digital service providers, as personal data has become the backbone of the modern digital economy.[1]

With the accelerating pace of automated processing, the widespread use of artificial intelligence, and the integration of big data technologies into various aspects of life, there has been a growing need to enhance protections for individuals against what is known as algorithmic exploitation—the invisible tracking of their digital behaviour. In response to this transformation, the right to informational self-determination has emerged as a key legal and ethical response.

This right refers to an individual's ability to control their personal data: to understand how it is used, to grant or withhold consent, and to exercise rights such as objection, correction, or deletion when necessary.

This right has acquired a prominent status in European law, particularly through the General Data Protection Regulation (GDPR), which has established a comprehensive legal framework to guarantee this right and promote its practical implementation.[2]

1.1. Significance of the Study

Practical reality has shown that legislative protection—despite its apparent strength—does not necessarily translate into effective protection on the ground, as it faces increasing technical, regulatory, and judicial challenges. The gap between legal provisions and the actual practices of data controllers, along with the ineffectiveness of oversight mechanisms, constitutes the main obstacles to the realisation of this right.

1.2. Research Problem

The European legislator has established an unprecedented framework for protecting personal data in the context of its processing. Through this framework, data subjects have been granted specific rights, while data controllers and processors have been obligated to respect those rights and adhere to a range of strict conditions during data processing.[3]

1 Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (Houghton Mifflin Harcourt 2013) 16.

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) (Text with EEA relevance) [2016] OJ L 119/1.

3 Yves Poullet and others, *Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks: Information Self-Determination in the Internet Era: Thoughts on Convention No 108 for the Purposes of the Future Work of the Consultative Committee (T-PD)* (Council of Europe 2004) 6.

However, practical practices reveal clear gaps between the legal text and its implementation—whether at the level of data controllers or enforcement authorities. Therefore, it is essential to analyse the gap between the legal framework and actual practice.

1.3. Research Methodology

This study aims to examine the right to informational self-determination from two complementary perspectives. The first concerns its legal foundation and legislative development, while the second focuses on the challenges of its practical implementation in an evolving digital environment. To achieve this, the study analyses the provisions of the European regulation, reviewing judicial precedents, regulatory reports, and real-world practices that expose gaps in implementation. It also offers practical recommendations aimed at strengthening this right and achieving a balance between digital innovation and the protection of individuals' fundamental rights.

1.4. Study Outline

The research is divided into the following sections:

- The nature of the right to informational self-determination;
- The content of the right to informational self-determination;
- Practical challenges and ways to address them.

2 THE NATURE OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION

The right to privacy intersects with the right to informational self-determination in certain aspects, necessitating clarification of the potential confusion arising from this overlap. Therefore, this section examines the concept of the right to privacy to establish a definition of the right to informational self-determination. The section concludes by identifying the legal nature of this right.

2.1. The Concept of the Right to Privacy

The term "privacy" does not appear explicitly in most Arab constitutions; instead, they typically refer to the concept of "private life".[4] Similarly, some legal systems—such as the French Civil Code—explicitly use the term private life, but without providing a precise definition.[5]

The earliest attempt to define human privacy and the right to its protection can be traced back to a well-known definition in American jurisprudence: "the right to be let alone."[6] However, this definition is criticised for its lack of legal criteria to determine what constitutes private life or the situations in which a person must be left alone. It is essential, therefore, to establish clear standards that govern the relationship between the individual and society, which would help delineate the personal sphere that one seeks to keep out of public view.

Among the modern attempts to define the right to privacy is the notion that it encompasses "our right to retain a private domain, which includes everything that forms part of us—such as the body, home, property, thoughts, emotions, secrets, and identity. The right to privacy gives us the ability to choose which parts of this domain others may not access, and to control the extent, method, and timing of the use of any elements we decide to disclose."[7]

4 Constitution of the United Arab Emirates [1971] Official Gazette 1. Article 31 of the UAE Constitution guarantees the freedom and confidentiality of postal, telegraphic, and other forms of communication, in accordance with the law. Article 36 provides for the inviolability of homes, prohibiting their entry without the consent of their occupants except in accordance with the law and in cases specifically outlined therein.

Similar provisions can be found in Article 10 of the Jordanian Constitution, Article 57 of the Egyptian Constitution, Article 24 of the Tunisian Constitution, Article 14 of the Lebanese Constitution, Article 36 of the Syrian Constitution, Article 38 of the Kuwaiti Constitution, and Article 47 of the Algerian Constitution.

Notably, the Algerian Constitution includes an additional provision in the final paragraph of the aforementioned article concerning personal data: "The protection of natural persons in the context of processing personal data is a fundamental right guaranteed by law, and violations thereof shall be punishable." See, Constitution of the People's Democratic Republic of Algeria 1989 (rev 2020), art 47 <https://www.constituteproject.org/constitution/Algeria_2020> accessed 20 March 2025.

5 Article 9 of the French Civil Code stipulates the right of every individual to respect for their private life: "Chacun a droit au respect de sa vie privée." See, Code Civil 1970 (rev 2025), art 9 <https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419288> accessed 20 March 2025. For a detailed discussion, see: Mamdouh Khalil Al-Bahr, *Protection of Private Life in Criminal Law* (Dar Al-Nahda Al-Arabiya 2011) 39 et seq.

6 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193, 195, doi:10.2307/1321160. 193,195.

This definition is attributed to the American judge Thomas M. Cooley. The term "privacy" in English corresponds to the Arabic term (*khususiyya*). According to the Arabic dictionary *Al-Mu'jam Al-Wasīt*, khususiyya refers to the specific or distinctive characteristic of a thing.

7 Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984) doi:10.1017/CBO9780511625138.

This definition relies on a subjective perspective in determining the components of the right to privacy, meaning that its scope may expand or contract depending on the view of the person formulating the definition.

Some have expanded the definition of privacy to the point of equating it with the concept of freedom. One such view holds that privacy is: *"for a person to live as they please, enjoying the practice of certain private activities—even if their behavior is in plain sight—such as choosing how to dress, appearing in a way that reflects one's personal identity, or riding a motorcycle without wearing a helmet."*[8]

This definition equates privacy with an individual's freedom to make personal, intellectual, and behavioural choices in both private and public life. However, such conflation is inaccurate. There is a clear distinction between the freedom of will that allows a person to make life choices in general and the right to define a private sphere that one wishes to shield from intrusion.

This conceptual confusion—between free will, human dignity, the right to form a family, and the concept of privacy or private life—is also seen in other definitions. For example, U.S. Supreme Court Justice Douglas defined privacy as "an individual's right to choose personal conduct and behaviour in life when engaging socially with others."[9]

This view links privacy to bodily dignity and the freedom from coercion and oppression.[10]

Those who adopt this broad concept believe that the right to privacy stems from the human right to liberty and self-autonomy.[11] On the other hand, there are those who limit the right to privacy to a distinct legal right that protects the individual from both material and moral intrusions into their private life. This view holds that: "Privacy is the right to protect one's personality from intrusion, and to safeguard individual independence, dignity, and personal integrity." [12]

It is evident that arriving at a comprehensive and precise definition of the right to privacy is highly challenging.[13] There are theoretical challenges in defining privacy itself, as it is

8 John H F Shuttuck, *Rights of Privacy* (To protect these rights, National Textbook Co 1977) 12-24.

9 Luara Karman, 'The Promise and Peril of Privacy' (1994) 22(4) Reviews in American History 725, doi:10.2307/2702826; David J Garrow, *Liberty and Sexuality: The Right to Privacy and the Making of Roe v Wade* (Macmillan 1994).

10 Alan F Westin, *Privacy and Freedom* (Atheeum 1967) 23.

11 Beate Roessler, 'Privacy as a Human Right' (2017) 117(2) Proceedings of the Aristotelian Society 187.

12 Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984) 156, doi:10.1017/CBO9780511625138.007.

13 Xueping Liu, 'Legal Dilemma and Outlet of Privacy Protection in the Era of Big Data' in Chuanchao Huang, Yu-Wei Chan and Neil Yen (eds), *2020 International Conference on Data Processing Techniques and Applications for Cyber-Physical Systems* (Advances in Intelligent Systems and Computing 1379, Springer 2021) 775, doi:10.1007/978-981-16-1726-3_95.

not a purely legal concept but rather one with intertwined psychological, social, political, and cultural dimensions. These difficulties are further compounded by the fact that the right to privacy encompasses numerous values and interests that are protected under various legal frameworks.

For this reason, some have argued[14] for the abandonment of the notion of a distinct right to privacy, asserting that the interests it protects are already safeguarded by different legal mechanisms across multiple laws. For instance: constitutions protect the right to private life by prohibiting unlawful intrusion into homes and telephone communications; criminal law protects individuals from physical assaults, unauthorized home entry, and defamation; civil law safeguards one's property rights, financial interests, and personal rights, as well as ensures peace at home through neighborhood regulations; and copyright law protects an author's right to decide when and how to publish their works. From this perspective, the interests forming the right to privacy are already protected, thereby eliminating the need to establish a separate and independent legal protection for privacy.

Most jurists,[15] however, hold a different view. They argue that the right to privacy warrants independent legal protection, based on the following considerations:

1) Existing legal provisions leave certain interests unprotected. For example, criminalising defamation and slander is intended to prevent the spread of false information, but it does not grant a person the right to prevent the dissemination of true information about themselves that they may not wish to be shared. Similarly, someone may be able to look into another person's home or its surroundings without physically entering it. Moreover, the collection of personal data such as name, phone number, address, or national ID number—without any misuse—does not necessarily constitute a violation of privacy or human dignity.

2) When dividing the right to privacy into components protected under different laws, it becomes difficult to establish appropriate rules for privacy protection that could apply to any violation. Furthermore, the scattered legal provisions across various legislations—often claimed to protect different aspects of privacy—are based on varying legislative considerations, which may not necessarily serve the interests that the right to privacy seeks to safeguard. For instance, the crime of insult or defamation mentioned earlier protects values such as dignity and honour, which are unrelated to the concept of privacy as intended here.

14 William M Beaney, 'The Right to Privacy and American Law' (1966) 31(2) Law and Contemporary Problems 253. Also see: Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Wolters Kluwer 2002).

15 Hamdi Abdel Rahman, *Rights and Legal Statuses* (Dar Al-Fikr Al-Arabi 1975) 17; Mahmoud Abdel Rahman Mohamed, *The Scope of the Right to Private Life (or Privacy): A Comparative Study* (Dar Al-Nahda Al-Arabiya 1994) 129; Al-Bahr (n 5) 39 et seq; Fred H Cate, *Privacy in the Information Age* (Mohamed Mahmoud Shehab tr, Al-Ahram Center for Translation and Publishing 1999) 33 et seq.

Despite the disagreements over how to define and conceptualise the right to privacy, the protection of an individual's private information remains a common denominator among all views and perspectives. This is what necessitates an exploration of informational privacy, which constitutes the essence of the right to informational self-determination—the subject of this study.

2.2. Definition of Informational Self-Determination

The historical roots of addressing informational privacy can be traced back to the work of Alan Westin in his book *Privacy and Freedom*, where he defines informational privacy as "the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others."[16] Similarly, Arthur Miller defines informational privacy as "the ability of individuals to control the circulation of information relating to them."[17]

The term "*informational self-determination*" originates from the efforts of certain German legal scholars as they discussed the right to be forgotten (i.e., the right to request the deletion of personal data) and the possibility of establishing a constitutional or legal foundation for it. Some German scholars argue that both the German Constitution and the rulings of the German Federal Constitutional Court provide a basis for the concept of informational self-determination. This is primarily grounded in the right to personal development, as stipulated in Article 2/1 of the German Basic Law.[18]

The rights to personality and privacy also embody the notion of human dignity in the sense of autonomous self-determination. The concept of human dignity entails that every individual has the right to decide the time, place, and nature of their actions in any given situation—including decisions regarding the disclosure of any type of personal data.

Such a conceptualisation has not remained merely academic or philosophical. It has been judicially affirmed and articulated in key constitutional jurisprudence. A landmark example is found in the reasoning of the Federal Constitutional Court of Germany, which clearly linked the protection of informational self-determination with the core constitutional values of human dignity and personal autonomy: "Technological developments concerning the modern processing of data have become so complex that the average citizen is no longer capable of understanding them. The hierarchy of values enshrined in the Constitution

16 Westin (n 10) 40.

17 Arthur R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press 1971) 33.

18 Claudia Kodde, 'Germany's "Right to be forgotten"' – between the Freedom of Expression and the Right to Informational Self-Determination' (2016) 30(1-2) International Review of Law, Computers & Technology 19, doi:10.1080/13600869.2015.1125154.

prioritises the worth and dignity of the individual as a member of a free society who determines his personal destiny. In particular, the general right of personality aims to protect this constitutional order when new threats emerge due to recent developments affecting these constitutional values."[19]

The right to informational self-determination can thus be defined as an individual's authority to control and manage their personal data in the context of digital processing arising from a contractual or legal relationship.

2.3. The Legal Nature of the Right to Informational Self-Determination

The concept of the right to privacy has served as the foundation for highlighting that the protection of personal data is a common denominator across all attempts to define the notion of privacy.

Clearly, the right to privacy is predominantly concerned with preventing others from accessing what an individual chooses to keep hidden. However, the protection of individuals in the context of processing their personal data constitutes a more interactive right. It presumes that such data is not inherently concealed but, rather, that those who process it are bound by legal obligations toward the data subject. In this sense, the right to informational self-determination arises from a legal or contractual relationship between the data subject and the entity processing the data.

Thus, despite the conceptual disagreements surrounding it, the right to privacy primarily aims to protect aspects of life that individuals wish to keep confidential, regardless of where the boundaries of such confidential aspects are drawn. It intersects with the right to informational self-determination in that one of the powers vested in the latter is the right to consent to data processing as well as the right to request data deletion. However, they diverge in terms of the interests they protect and the mechanisms of protection.

The right to privacy safeguards an individual's interest in leading a peaceful life free from external intrusion, granting the ability to keep personal facts and data confidential. It is fundamentally a negative, prohibitive right that seeks to prevent others from accessing certain areas of a person's life. In contrast, informational privacy—or the right to informational self-determination—extends protection to individuals both in a state of passivity and activity, so to speak. It empowers individuals to choose whether to disclose their personal data, to restrict its processing, or to request its deletion once the purpose for

19 ibid 30.

processing has ceased to exist, even if the disclosure or processing of such data does not infringe on their privacy per se.

Referring to Recital 1 of the General Data Protection Regulation (GDPR), it states that: "The protection of natural persons in relation to the processing of personal data is a fundamental right."[20] This is grounded in Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter)[21] and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), both of which affirm that "Everyone has the right to the protection of personal data concerning him or her."[22]

Everyone has the right to respect for his or her private and family life, home and communications. Public authorities shall not interfere with the exercise of this right except in accordance with the law and where necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[23]

Accordingly, the right to informational self-determination, i.e., the protection of personal data, is recognised as a fundamental human right under the aforementioned legal frameworks.

3 THE CONTENT OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION

The Regulation outlines several rights to which data subjects are entitled. These include the right to access one's processed data, the right to data portability, the right to rectification, the right to erasure (the right to be forgotten), the right to restriction of processing, the right to object to data processing, and the right to prevent automated decision-making. Each of these will be discussed in turn.

20 Regulation (EU) 2016/679 (n 2) recital 1.

21 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

22 Treaty on the Functioning of the European Union of 13 December 2007 (consolidated version) [2016] OJ C 202/47.

23 Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 November 1950) [1955] UNTS 213/222, art 8.

3.1. Rights of the Data Subject During Processing [24]

3.1.1. The Right of Access by the Data Subject

The right of access applies to the controller who falls within the scope of the Regulation. This obligation imposed on the controller requires enabling data subjects to access their data, along with all necessary information related to the processing of such data.

This right is an effective tool that allows individuals to access vast amounts of data being processed about them by various institutions and companies.[25]

Under this right, the data subject, upon request, must be promptly informed whether their personal data is being processed by the controller or a processor acting on behalf of the controller. The data subject is not required to provide any justification for making this request.[26]

The UK Supreme Court has ruled that: "The controller is obliged to make reasonable and proportionate efforts to search for the information requested by the data subject. However, such a search must not consume all the controller's time and effort. It is not necessary—according to the Court—for the controller to leave no stone unturned' to fulfil the request."[27]

The burden of proof that a request is manifestly unfounded or excessive lies with the controller, as the data subject is exercising a legitimate right. Whoever alleges abuse or misuse of this right must bear the burden of proving it.

3.1.2. Scope of the Right

This right grants the data subject the ability to know whether their personal data is being processed or not, and whether the processing is carried out by the controller or by a

24 Here, we assume that the data processing takes place under two scenarios: first, processing based on a legitimate legal interest carried out by a public institution, in accordance with the purposes permitted by the Regulation without requiring the prior consent of the data subject; and second, processing based on prior consent, in which case the consent must be explicit, specific, informed, and based on a clear affirmative action by the user. Pre-ticked checkboxes do not constitute valid consent under the General Data Protection Regulation (GDPR) and the E-Privacy Directive.
Bundesverband der Verbraucherzentralen und Verbraucherverbande - Verbraucherzentrale Bundesverband eV v Planet49 GmbH C-673/17 [2020] 1 CMLR 25; [2019] 9 WLUK 540 (ECJ (Grand Chamber)). For more details see: Klaus Wiedemann, 'The ECJ's Decision in Planet 49 (Case C-673/17): A Cookie Monster or Much Ado About Nothing?' (2020) 51(4) International Review of Intellectual Property and Competition Law 543, doi:10.1007/s40319-020-00927-w.

25 Regulation (EU) 2016/679 (n 2) art 15.

26 *Deer v University of Oxford* [2017] EWCA (Civ) 121.

27 *Ezsias v Welsh Ministers* [2007] AII ER (D) 65. The Supreme Court applied the provisions of the UK Data Protection Act 1998, which was inspired by the previous European Directive of 1995. This directive granted individuals the right to access their processed data, particularly to ensure the accuracy of the data and the lawfulness of its processing. "….in order to verify in particular, the accuracy of the data and the lawfulness of the processing".

processor acting on their behalf. The data subject must also be granted access to their data and informed of the relevant information concerning its processing.[28]

The rationale behind this right, as stated in the Regulation, is to ensure that the data subject is *"aware of and able to verify the lawfulness of the processing."*[29]

In *Durant v. Financial Services Authority*, the British Court of Appeal emphasised that the purpose of allowing individuals to access their personal data is to enable them to assess whether the controller's processing is unlawful or infringes upon their privacy. If that is the case, the data subject has the right to take the necessary measures to protect their rights.[30]

The data cannot be withheld from the data subject on the grounds that it is already known to them or that it was initially obtained from them.[31] The case law of the Court of Justice of the European Union affirms that the right of access to personal data must be interpreted as including, upon request by the data subject, the identification of the specific recipients to whom the personal data have been disclosed. This right may not be limited by the data controller to merely providing information about categories of recipients, except in two exceptional cases:

1. When it is physically impossible to provide information on the specific recipients, for example, if they have not yet been identified.
2. When the request is manifestly unfounded or excessive, pursuant to Article 12(5) of the General Data Protection Regulation (GDPR).

Empowering individuals to know the specific recipients of their data enhances their ability to exercise other rights—such as rectification, erasure, or objection to processing—and reinforces the principle of transparency in personal data processing.[32]

Moreover, a controller who collects data from publicly available sources must still ensure the accuracy of such data and maintain transparency toward the data subjects, even if the information is accessible to the public.[33]

28 Regulation (EU) 2016/679 (n 2) art 15, para 1 (a)-(h); Guidelines 01/2022 On Data Subject Rights - Right Of Access (adopted 28 March 2023, version 2.1) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en> accessed 20 March 2025.

29 Regulation (EU) 2016/679 (n 2) recital (63).

30 *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

31 The proper purpose of a subject access request is to enable a data subject to check the accuracy of the data and to see that they are being processed lawfully, see: *Dr Cécile Deer v The University of Oxford* [2017] EWCA Civ 121; *Durant v Financial Services Authority* (n 30); *Johnson v Medical Defence Union* [2007] EWCA Civ 262.

32 *RW v Österreichische Post AG* C-154/21, Opinion of Advocate General Pitruzzella (ECJ, 9 June 2022) ECLI:EU:C:2022:452.

33 Case No TD/00263/2020, Decision No R/00214/2021 (Spanish Data Protection Authority, 28 May 2021).

On the other hand, the right of access under Article 15 of the GDPR does not include a general right to inspect the files of tax authorities.[34]

When a person's data is linked to others such as information related to several tenants of a building, a report written by someone about another person in a professional capacity, or a complaint filed by one colleague against another within an institution—the controller must provide only the data pertaining to the requesting data subject, while withholding any data related to others.[35]

3.2. The Right to Data Portability

This right is closely linked to the right of access to data. It entitles the data subject to receive the personal data they have provided to the controller in a structured, commonly used, and machine-readable format, and to transmit that data to another controller. This right aims to facilitate the ability of data subjects to transfer and transmit their data from one IT system to another and to switch between service providers.[36]

The right to data portability is subject to the technical feasibility of implementation, and it does not apply when a public authority processes personal data in the performance of a task carried out in the public interest.

The technical feasibility of its implementation restricts the right to data portability. It cannot be exercised when a public authority processes personal data in the performance of a task carried out in the public interest. It is essential to strike a balance between the protection of personal data and the European Union's objective of enhancing data mobility and accessibility, which supports the achievement of the EU Data Strategy.

This requires balancing the legal standards set by the General Data Protection Regulation (GDPR)—which aim to protect data subjects—to encourage the availability, access, and reuse of data by market actors to promote sustainable growth and innovation within the data economy and society. This vision is further supported by more recent legislative instruments such as the Digital Markets Act (DMA) of 2022 and the Data Act (DA) of 2023.[37]

3.3. The Right to Rectification

The Regulation grants data subjects the right to have their personal data rectified if it is inaccurate or incomplete. This right is closely tied to the controller's and processor's obligation to take all reasonable steps to ensure the accuracy of personal data. When this right is exercised, the controller is required to inform any recipient of the data—such as employees, processors, or any third parties to whom the data has been disclosed—about the

34 Judgment No 15 K 1212/19 (Financial Court of Munich, 3 February2022).
35 Case No ROT 19/4649 (District Court Rotterdam, 22 March 2021).
36 Regulation (EU) 2016/679 (n 2) art 16.
37 Case No ROT 19/4649 (n 35).

rectification, unless this proves impossible or involves disproportionate effort in relation to the importance of the rectification. Furthermore, the data subject must be informed about all those parties who have had access to their data. In this regard, the Court of Justice of the European Union indicated that the assessment of the accuracy and completeness of such data must be made in light of the purpose for which it was collected.[38]

3.4. The Right to Object to Data Processing

Every data subject has the right to object to the processing of their personal data in certain cases.[39] For instance, this right is absolute when the data is being processed for direct marketing purposes. In such a case, the controller who receives an objection from a data subject must cease processing the data for marketing purposes. There are no exceptions or limitations for the data subject when exercising this right in that context.

The Court of Justice of the European Union affirmed that purely commercial interests may constitute a "legitimate interest" under Article 6(1)(f) of the General Data Protection Regulation (GDPR). This ruling clarifies that such interests do not need to be explicitly defined by law to be considered legitimate. A "legitimate interest" is not confined to public, moral, or security-related matters but also encompasses objectives related to ordinary commercial activity.[40]

The data subject's right to accept or refuse the processing of their personal data intersects with competition law, as illustrated by a ruling of the German Federal Court of Justice, which upheld a decision by the Federal Cartel Office. The office had found that Facebook abused its dominant position in the German social media market by imposing terms of use requiring users to consent to the collection and merging of their data from external sources (such as Instagram, WhatsApp, and third-party websites and applications) with their Facebook profiles—without offering users a genuine option to refuse.[41]

Furthermore, the violation of a data subject's rights does not automatically entitle them to compensation unless they had suffered actual harm as a result of the violation.[42]

38 *VP v Országos Idegenrendészeti Foigazgatóság* C-247/23 [2025] 4 WL.R 50; [2025] 3 WLUK 209 (ECJ (1st Chamber)).

39 Regulation (EU) 2016/679 (n 2) art 5, para 1.

40 *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* C-621/22 (ECJ (9th Chamber), 4 October 2024) ECLI:EU:C:2024:858.

41 The German Federal Supreme Court's interim decision in the abuse of dominance proceedings, *Bundeskartellamt v Facebook* Case KVR 69/19 (BGH, 23 June 2020). For more details: Klaus Wiedemann, 'A matter of choice: the German Federal Supreme Court's interim decision in the abuse of dominance proceedings *Bundeskartellamt v Facebook* (Case KVR 69/19)' (2020) 51(9) International Review of Intellectual Property and Competition Law 1168, doi:10.1007/s40319-020-00990-3. *UI v Österreichische Post AG* C-300/21 [2023] 1 WLR 3702; [2023] 5 WLUK 22 (ECJ (3rd Chamber)).

42 *UI v Österreichische Post AG* (n 41).

3.5. The Right to Object to Direct Marketing

This right allows the data subject to request that the controller stop using their data for direct marketing purposes. It also includes the authority to object to any profiling attempts that aim to determine the data subject's interests, preferences, and inclinations.[43]

This right covers all forms of direct marketing and any attempts to use personal data for marketing purposes across various media—whether through personal communication via regular mail or email, fax, SMS, or online advertising.

Therefore, the data subject's objection must be comprehensive and cover all forms of processing across all types of communication media. For example, it is not sufficient to object only to email messages unless the data subject clearly states that they object to all forms of processing through all media.

It is worth noting that the absence of an objection by a specific person to receiving marketing materials does not necessarily mean that sending such materials to that person is lawful.

The right applies to all personal data processed for the purposes of direct marketing. Although the Regulation does not explicitly define *direct marketing*, it is generally understood to refer to all advertising and promotional materials directed at a specific recipient.

A broad concept of direct marketing has been adopted in the United Kingdom, defining it as any purposeful communication from an organisation to an individual that conveys the goals and values of the organisation. This concept has been further expanded to include political election campaigns as well as communication from charitable organisations directed at potential donors to inform them of their activities.[44]

This right is not limited to rejecting the receipt of marketing materials but also extends to all preceding activities related to sending marketing materials, such as data collection, profiling, sorting of data, etc.[45] The right to object to the use of personal data for direct marketing purposes is absolute, with the Regulation imposing no restrictions or exceptions.

3.6. The Right to Request Erasure (Right to be Forgotten)

According to Article 17 of the Regulation, the data subject has the right to request the data controller to erase the personal data concerning him or her without undue delay. The controller is obliged to erase the personal data in the following cases:

1) If the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.[46]

43 Regulation (EU) 2016/679 (n 2) art 21.

44 Peter Carey, *Data Protection: A Practical Guide to UK Law* (5th edn, OUP 2018) 141.

45 ibid 142.

46 Regulation (EU) 2016/679 (n 2) art 17, para 1 (a).

2) If the data processing was based on the data subject's prior consent.[47]
3) If the data subject objects to the processing, and there are no overriding legal grounds to justify it.[48]
4) If the personal data were processed unlawfully.[49]
5) If the controller is under a legal obligation to erase the personal data.[50]
6) If the personal data were collected in relation to the offer of information society services as referred to in Article 8(1).[51]

The data controller is required to comply with the erasure request in the aforementioned cases, even if the continued processing does not cause harm to the data subject.

It is incumbent upon the data controller to determine the purposes for which personal data is collected and processed in a manner that is clear, legitimate, adequate, relevant, and limited to what is necessary for the purposes of processing.[52]

Accordingly, the data subject has the right to request the deletion of their data from the controller's records if the controller violates these conditions. This also applies if the period during which the data was retained exceeds what is necessary to fulfil the declared purposes of processing.

Further processing for archiving and documentation in the public interest, or for scientific, historical, or statistical research purposes, is considered one of the exceptions recognised by the Regulation.

To ensure that the purpose of the further processing is compatible with the original purpose(s) for which the data was initially processed, the controller—after fulfilling all legal requirements of the original processing—must take into account the following considerations:[53]

1) Any link between the intended further processing and the original processing.
2) The context in which the personal data was collected, particularly the reasonable expectations of the data subject based on their relationship with the controller regarding further use of the data.

47 ibid, art 17, para 1 (b).
48 ibid, art 17, para 1 (c).
49 ibid, art 17, para 1 (d).
50 ibid, art 17, para 1 (e).
51 ibid, art 17, para 1 (f).
52 According to a 2009 survey, nearly 80 percent of employers use search engines to look up job applicants, and it was found that most employers reject candidates based on what they discover in their online history. More than half of the employers reported that they would reject a candidate due to "concerns about the candidate's lifestyle," "inappropriate comments or text written by the candidate," or "inappropriate pictures, videos, or information." These results are typically generated by private companies that rank job applicants based on their social media profiles and Google search results. For more details see: Shlomit Yanisky-Ravid, 'To Read or Not to Read: Privacy Within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory' (2014) 64(1) American University Law Review 65-6.
53 Regulation (EU) 2016/679 (n 2) art 9, para 2 (j).

3) The existence of appropriate safeguards in both the original and the subsequent processing operations.
4) Whether the processing is based on the data subject's consent or a legal basis under Union law or the law of a Member State.
5) Even if the further processing is not compatible with the original purpose, it may still be lawful if it is deemed a necessary and appropriate measure to safeguard objectives serving the public interest, provided that the principles laid down in the Regulation are observed, most importantly, the data subject's right to object.

Furthermore, it is considered lawful for the controller to indicate the likelihood of criminal activity or threats to public security, thereby justifying the transfer of personal data—whether in individual or collective cases—to a competent authority. However, such data transfers or further processing must be prohibited if they are not aligned with a legal, professional, or confidentiality obligation.[54]

When the processing is based on the data subject's consent, the controller must be able to demonstrate that the data subject has indeed given consent to the processing of their personal data.[55]

The data subject has the right to withdraw their consent at any time. Such withdrawal does not affect the lawfulness of the processing carried out prior to the withdrawal. Before giving consent, the data subject must be informed of their right to withdraw it, and the withdrawal process must be as simple as the process for granting consent.[56]

The data subject may revoke their consent to the processing of their data for a specific purpose or purposes, especially where there is no other legal basis for retaining the data under processing. The Regulation explicitly prohibits the processing of sensitive personal data, unless the data subject consents to such processing for one or more specific purposes.[57]

Where the data subject objects to the processing[58] of their personal data due to the absence of overriding legal grounds for such processing, or where the processing is aimed at

54 ibid, recital (50).

55 ibid, art 7, para 1.

56 ibid, art 7, para 4.

57 ibid, art 9, para 1. **Sensitive Date:** Sensitive personal data refers to any information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data used for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation.

58 ibid, art 21. Pursuant to paragraph (1) of Article 21, where there are no overriding legal grounds for processing, or where the data subject has objected to processing in accordance with paragraph (2) of Article 21—which provides that the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling.

profiling,[59] the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims.[60]

The data controller must erase personal data in compliance with a legal obligation imposed under Union law or the law of a Member State to which the controller is subject.

If the processing is carried out in compliance with such a legal obligation or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, such processing constitutes a lawful basis.

Processing of personal data is also considered lawful when it is necessary for the protection of vital interests of the data subject or of another natural person—such processing should, in principle, take place only when no other legal basis is available.

Processing is also deemed lawful when it is carried out for the purposes of preventing or mitigating threats to network and information system security or addressing such threats.

Where personal data are collected in relation to the direct offer of information society services to a child, such processing is lawful if the child is at least 16 years old. If the child is under the age of 16, processing is lawful only if consent is given or authorised by the holder of parental responsibility for the child.

When the controller has made personal data public and is subsequently required to erase it, the controller shall, taking into account available technology and the cost of implementation, take reasonable steps including technical measures to inform other controllers or processors processing the personal data that the data subject has requested the erasure of any links to, or copies or replications of, those personal data.

Consent of the data subject is not required for processing in the following cases:

1) When processing is carried out in the context of exercising the right to freedom of expression and information.

59 Profiling: the recording and analysis of an individual's psychological and behavioral characteristics in order to assess or predict their capabilities in a certain area, or to assist in classifying them into specific categories. See: *Oxford Reference* <https://www.oxfordreference.com/display/10.1093/oi/authority.20111123105355319> accessed 20 March 2025.

60 Regulation (EU) 2016/679 (n 2) art 6, para 1. The aforementioned points—(e) and (f) of Article 6(1)—state that processing is lawful if: it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, **or** it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, especially where the data subject is a child.

2) When processing is required for compliance with a legal obligation imposed by Union or Member State law to which the controller is subject.
3) When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, particularly for reasons of public interest in the area of public health.
4) When processing is carried out for archiving purposes in the public interest, or for scientific or historical research purposes, or for statistical purposes.
5) When processing is necessary for the establishment, exercise, or defence of legal claims.

4 PRACTICAL CHALLENGES AND WAYS TO ADDRESS THEM

4.1. Practical Challenges

4.1.1. The Limitations of Consent in AI and Big Data Environments

The General Data Protection Regulation (GDPR) heavily relies on explicit consent as a legal basis for data processing. However, this basis faces fundamental challenges in contexts driven by algorithms, big data, artificial intelligence, social media, and similar technologies—where individuals often lack the capacity to fully understand or effectively control all aspects of how their data is used. As a result, consent may be rendered practically meaningless.[61] Additionally, algorithmic biases and automated decisions can occur without the individual's ability to intervene or effectively object.[62]

61 See for further detail: Varda Mone and CLV Sivakumar, 'An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies' (2022) 22(3) Legal Information Management 166, doi:10.1017/S1472669622000317.

62 Regulation (EU) 2016/679 (n 2) arts 22, 13, 15. Although Article 22 of the General Data Protection Regulation (GDPR) is intended to protect individuals from decisions made without human intervention, its practical interpretation significantly narrows the scope of protection. The provision is interpreted restrictively to apply only to decisions that are fully automated and produce legal effects or similarly significant outcomes. As a result, many AI-based applications fall outside the scope of the prohibition, despite their real-world impact on individuals. Moreover, the transparency requirements set out in Articles 13 to 15 of the GDPR do not effectively guarantee what is referred to as a "meaningful explanation." The GDPR does not oblige data controllers to provide a detailed account of the logic behind automated decisions but merely requires a general description of the nature of the processing. This weakens individuals' ability to challenge outcomes or demand their correction. See for further detail: Adrienn Lukács and Szilvia Váradi, 'GDPR-Compliant AI-Based Automated Decision-Making in the World of Work' (2023) 50 Computer Law & Security Review 4, doi:10.1016/j.clsr.2023.105848.

4.1.2. Difficulties in Exercising Individual Rights

Although individual rights are legally enshrined, their actual exercise faces several obstacles, including:

- The complexity of digital forms for submitting access or erasure requests,[63]
- The ambiguity surrounding the identity of the actual data controller, particularly in cases of joint processing.[64]

4.1.3. The Problem of Centralised Enforcement and Institutional Performance Disparities

Practical implementation reveals significant disparities in the effectiveness of data protection authorities across EU member states. Major cases, such as Schrems I and Schrems II,[65] along with regulatory reports, have highlighted occasional weaknesses in cooperation between national supervisory authorities.

4.1.4. The Protection of Mental Data and Emerging Data Patterns

With the advancement of neurotechnology and brain–computer interfaces (BCIs), a new category of data has emerged, referred to as *mental data*. This type of data originates directly from mental activity and includes emotions, beliefs, attitudes, and even intentions prior to their behavioural expression.[66]

63 See for further detail: Junkai Ding and Xiaoyan Quan, 'Legal Challenges in Protecting Personal Information in Big Data Environments' (*SSRN*, 5 March 2025) <http://dx.doi.org/10.2139/ssrn.5166908> accessed 20 March 2025.

64 See for further detail: Mone and Sivakumar (n 61) 170. For example, it is difficult to identify who is liable for harm caused to individuals whose data is used by Internet of Things (IoT) devices or through big data analytics and algorithms.

65 *Maximilian Schrems v Data Protection Commissioner* C-362/14 (ECJ (Grand Chamber), 6 October 2015) ECLI:EU:C:2015:650. Schrems, an Austrian privacy activist, filed a complaint against Facebook Ireland on the grounds that the personal data of European users was being transferred to the company's servers in the United States. This transfer was carried out under the "Safe Harbor" agreement between the European Union and the United States. Schrems argued that the U.S. does not provide an adequate level of data protection, especially in light of Edward Snowden's revelations about American surveillance programs such as PRISM. The Court of Justice of the European Union (CJEU) invalidated the Safe Harbor agreement, affirming that Member States cannot transfer citizens' data to a country that does not ensure a level of protection essentially equivalent to that guaranteed by fundamental rights such as privacy (*Data Protection Commissioner v Facebook Ireland & Maximillian Schrems Data Protection Commissioner v Facebook Ireland & Maximillian Schrems* C-311/18 (ECJ (Grand Chamber), 16 July 2020)). Following the annulment of Safe Harbor, a new agreement known as the "Privacy Shield" was established. Schrems challenged this agreement as well, arguing that U.S. surveillance practices remained in place and that EU citizens lacked effective legal remedies or avenues for complaint in the United States. The Court also invalidated the Privacy Shield, ruling that U.S. surveillance laws, such as FISA Section 702, do not provide a level of protection equivalent to that offered under EU law.

66 Marcello Ienca and Gianclaudio Malgieri, 'Mental Data Protection and the GDPR' (2022) 9(1) Journal of Law and the Biosciences lsac006, doi:10.1093/jlb/lsac006.

This emerging category raises unprecedented legal questions regarding the extent to which the General Data Protection Regulation (GDPR) applies to it, and whether existing legal instruments are sufficient to ensure its protection. It also challenges the ability of the European regulatory framework to address such data types, especially in the absence of clear legal rules governing neurotechnological measurement or direct interaction with the human mind.

While mental data may fall under the category of *sensitive data* as defined in Article 9 of the GDPR, its intangible and involuntary nature introduces novel legal challenges. A key concern is that such data are often generated and collected without the full awareness of the data subject, thereby undermining the effectiveness of consent as a legal safeguard.

These challenges demonstrate the widening gap between the legal framework and real-world practices, underscoring the need to develop regulatory, interpretive, and technological tools capable of ensuring the meaningful enforcement of the right to informational self-determination—an issue to be analysed in the following section.

4.2. Proposed Approaches to Address Implementation Gaps

4.2.1. A Critical Analysis of the Gap Between Legal Text and Practice

While the General Data Protection Regulation (GDPR) represents a qualitative leap in the field of digital rights protection, reality reveals a clear gap between the content of legal provisions and their implementation mechanisms. The texts affirm the principle of individual sovereignty over personal data, yet in practice, individuals face significant obstacles in exercising this right—whether due to technical complexity or the reluctance of data controllers. Many digital interfaces do not offer genuine options for consent or objection, instead presenting them as mere formalities.

4.2.2. A Study of Judicial and Regulatory Cases

Several cases before the Court of Justice of the European Union (CJEU) have highlighted deficiencies in application, most notably:

1) The *Schrems II* case confirmed the inadequacy of safeguards in data transfers to the United States, leading to the invalidation of the Privacy Shield framework.
2) The *Google Spain* case established the "right to be forgotten" but faced technical difficulties in enforcement.
3) Recent decisions by national supervisory authorities—such as France's CNIL and Germany's BfDI—have shown divergences in interpretation and enforcement levels.

In the context of GDPR implementation, notable disparities have emerged between national authorities in the EU, particularly between France's Commission Nationale de l'Informatique et des Libertés (CNIL) and Germany's Federal Commissioner for Data

Protection and Freedom of Information (BfDI). CNIL adopted a strict approach early on, imposing a €50 million fine on Google in January 2019 for violating transparency principles and legal bases for processing, particularly concerning cookies.[67]

By contrast, BfDI initially demonstrated a more restrained approach, with some fines not exceeding €20,000. However, this stance shifted over time, especially in the case where BfDI imposed a fine of over €9.5 million on 1&1 Telecom due to insufficient security measures related to data access.[68]

This divergence reflects differences in the interpretation and implementation of the Regulation, as well as the discretionary power exercised by each authority. It also underscores the need for harmonised standards to ensure fair enforcement within the Digital Single Market.

4.2.3. Evaluating the Effectiveness of Oversight and Supervision

The success of the GDPR depends largely on the capacity of national supervisory authorities and the European Data Protection Board (EDPB) to operate in a coordinated and coherent manner. However, the multiplicity of entities and differences in regulatory capacities have resulted in disparities that affect fairness and effectiveness. The decentralised enforcement model, lacking binding authority at the EU level, weakens the Union's collective response to cross-border challenges.[69]

67 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million euros against Google LLC' (*EDPB*, 21 January 2019) <https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en> accessed 20 March 2025.

68 'BfDI Imposes Fines on Telecommunications Service Providers' (*EDPB*, 18 December 2019) <https://www.edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_en> accessed 20 March 2025.

69 Although the European Data Protection Board (EDPB) was established under Article 68 of the General Data Protection Regulation (GDPR) as a coordinating body intended to harmonize the application of data protection rules within the Digital Single Market, the structure of the European data protection system is not based on actual executive centralization. Instead, it operates under a decentralized model, in which each national authority oversees the application of the GDPR within its own territorial jurisdiction.
This distribution results in significant disparities in interpretation, enforcement speed, and the level of strictness applied. The EDPB does not possess direct supervisory or enforcement powers over national authorities; its authority is limited to issuing non-binding guidelines or making binding decisions only in cases of cross-border processing disputes, as set out in Articles 64–65 of the Regulation.
As a consequence, the absence of a binding federal-level executive authority undermines the practical effectiveness of the GDPR—particularly in addressing cross-border challenges such as global digital platforms or data transfers outside the European Union.
See in detail: *European Data Protection Board (EDPB)* <https://edpb.europa.eu > accessed 20 March 2025; Christopher Kuner, Lee A Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (CUP 2020).

4.2.4. Recommendations to Strengthen the Practical Application of the Right to Informational Self-Determination

1. Strengthen centralised enforcement within the EU by granting the EDPB quasi-judicial powers.

2. Improve user interface design to ensure genuine understanding of consent and data processing options.

3. Include mental data and emerging technologies in the category of special data under the GDPR.

4. Expand the application of Data Protection Impact Assessments (DPIAs) to advanced and automated models.

5. Require companies to review their algorithms to ensure respect for individual rights and to prevent algorithmic discrimination.

5 CONCLUSIONS

The right to informational self-determination is one of the most prominent digital rights to emerge from the profound transformations in data-driven societies. This study has demonstrated that the right is no longer merely an extension of the right to privacy, but has become a concrete expression of individual sovereignty in the digital space—a central safeguard for human dignity in the face of algorithms, automated technologies, and modern tracking systems.

The GDPR has introduced an advanced legislative structure, both in terms of its general principles and the rights it grants individuals. Yet, practical challenges in enforcement remain. From the limitations of consent mechanisms to difficulties in exercising rights and institutional disparities in enforcement, several obstacles undermine the effectiveness of the right to informational self-determination.

This research concludes that bridging the gap between legislation and implementation requires:

- Rethinking the institutional model for GDPR enforcement at the EU level.
- Updating legal provisions to keep pace with rapid technological developments, particularly concerning artificial intelligence and mental data.
- Adopting flexible regulatory tools that accommodate the dynamic nature of data processing environments.

The future of the right to informational self-determination depends on the EU's ability to combine legal rigour, technological adaptability, and societal awareness within a coherent framework that ensures this right's practical enforceability alongside its normative value.

REFERENCES

1. Al-Bahr MK, *Protection of Private Life in Criminal Law* (Dar Al-Nahda Al-Arabiya 2011).
2. Beaney WM, 'The Right to Privacy and American Law' (1966) 31(2) Law and Contemporary Problems 253.
3. Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' in Schoeman FD (ed), *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984) 156, doi:10.1017/CBO9780511625138.007.
4. Bygrave LA, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Wolters Kluwer 2002).
5. Carey P, *Data Protection: A Practical Guide to UK Law* (5th edn, OUP 2018).
6. Cate FH, *Privacy in the Information Age* (MM Shehab tr, Al-Ahram Center for Translation and Publishing 1999).
7. Ding J and Quan X, 'Legal Challenges in Protecting Personal Information in Big Data Environments' (*SSRN*, 5 March 2025) doi:10.2139/ssrn.5166908.
8. Garrow DJ, *Liberty and Sexuality: The Right to Privacy and the Making of Roe v Wade* (Macmillan 1994).
9. Ienca M and Malgieri G, 'Mental Data Protection and the GDPR' (2022) 9(1) Journal of Law and the Biosciences lsac006, doi:10.1093/jlb/lsac006.
10. Karman L, 'The Promise and Peril of Privacy' (1994) 22(4) Reviews in American History 725, doi:10.2307/2702826.
11. Kodde Cl, 'Germany's "Right to be forgotten"' – between the Freedom of Expression and the Right to Informational Self-Determination' (2016) 30(1-2) International Review of Law, Computers & Technology 17, doi:10.1080/13600869.2015.1125154.
12. Kuner C, Bygrave LA and Docksey C, *The EU General Data Protection Regulation (GDPR): A Commentary* (CUP 2020).
13. Liu X, 'Legal Dilemma and Outlet of Privacy Protection in the Era of Big Data' in Huang C, Chan YW and Yen N (eds), *2020 International Conference on Data Processing Techniques and Applications for Cyber-Physical Systems* (Advances in Intelligent Systems and Computing 1379, Springer 2021) 775, doi:10.1007/978-981-16-1726-3_95.
14. Lukács A and Váradi S, 'GDPR-Compliant AI-Based Automated Decision-Making in the World of Work' (2023) 50 Computer Law & Security Review 1, doi:10.1016/j.clsr.2023.105848.
15. Mayer-Schönberger V and Cukier K, Big Data: A Revolution That Will Transform How We Live, Work, and Think (Houghton Mifflin Harcourt 2013).
16. Miller AR, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press 1971).

17. Mohamed MAR, *The Scope of the Right to Private Life (or Privacy): A Comparative Study* (Dar Al-Nahda Al-Arabiya 1994).

18. Mone V and Sivakumar CLV, 'An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies' (2022) 22(3) Legal Information Management 166, doi:10.1017/S1472669622000317.

19. Poullet Y and others, *Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks: Information Self-Determination in the Internet Era: Thoughts on Convention No 108 for the Purposes of the Future Work of the Consultative Committee (T-PD)* (Council of Europe 2004).

20. Rahman HA, *Rights and Legal Statuses* (Introduction to Civil Law, Dar Al-Fikr Al-Arabi 1975).

21. Roessler B, 'Privacy as a Human Right' (2017) 117(2) Proceedings of the Aristotelian Society 187.

22. Schoeman FD (ed), *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984) doi:10.1017/CBO9780511625138.

23. Shuttuck JHF, *Rights of Privacy* (To protect these rights, National Textbook Co 1977).

24. Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193, doi:10.2307/1321160.

25. Westin AF, *Privacy and Freedom* (Atheeum 1967).

26. Wiedemann K, 'A matter of choice: the German Federal Supreme Court's interim decision in the abuse of dominance proceedings *Bundeskartellamt v Facebook* (Case KVR 69/19)' (2020) 51(9) International Review of Intellectual Property and Competition Law 1168, doi:10.1007/s40319-020-00990-3.

27. Wiedemann K, 'The ECJ's Decision in Planet 49 (Case C-673/17): A Cookie Monster or Much Ado About Nothing?' (2020) 51(4) International Review of Intellectual Property and Competition Law 543, doi:10.1007/s40319-020-00927-w.

28. Yanisky-Ravid S, 'To Read or Not to Read: Privacy Within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory' (2014) 64(1) American University Law Review 53.

AUTHORS INFORMATION

Najlaa Flayyih*
PhD (Law), Associate Professor, College of Law, Ajman University, Ajman, United Arab Emirates
n.flayyih@ajman.ac.ae
https://orcid.org/0000-0002-2807-9350
Corresponding author, responsible for research methodology, data curation, investigation, writing-original draft.

Mohammed Hasson Ali
PhD (Law), Associate Professor in Private Law, Law Faculty, University of Fujairah, Fujairah, United Arab Emirates
mohd.abdullah@uof.ac.ae
https://orcid.org/0000-0003-3592-2657
Co-author, responsible for data curation, funding acquisition, resources, validation, writing – review & editing.

Ahmad Fadli
PhD (Law), Associate Professor, College of Law, Ajman University, Ajman, United Arab Emirates
a.fadli@ajman.ac.ae
https://orcid.org/0000-0003-2117-7801
Co-author, responsible for conceptualization, formal analysis, validation, writing-original draft.

Khaled Aljasmi
PhD (Law), Associate Professor, College of Law, Ajman University, Ajman, United Arab Emirates
k.aljasmi@ajman.ac.ae
https://orcid.org/0000-0003-0085-8085
Co-author, responsible for formal analysis, data curation, validation, writing-original draft.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinions and views expressed in this manuscript are free of any impact of any organizations.

FUNDING ACKNOWLEDGMENT

Publication of this article is funded by authors.

RIGHTS AND PERMISSIONS

EDITORS

Managing editor – Mag. Yuliia Hartman. **English Editor** – Julie Bold.
Ukrainian language Editor – Lilia Hartman.

ABOUT THIS ARTICLE

Cite this article
Flayyih N, Hasson Ali M, Fadli A and Aljasmi K, 'The Right to Informational Self-Determination between Legislation and Implementation' (2025) 8(3) Access to Justice in Eastern Europe 362-89 <https://doi.org/10.33327/AJEE-18-8.3-a000116>

DOI: https://doi.org/10.33327/AJEE-18-8.3-a000116

Keywords: *personal data protection, informational self-determination, data subject rights, informational privacy, GDPR.*

DETAILS FOR PUBLICATION

Date of submission: 08 May 2025
Date of acceptance: 02 Jul 2025
Online First publication: 21 Jul 2025
Last Publication: 18 Aug 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with minor revisions

Technical tools were used in the editorial process
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ПРАВО НА ІНФОРМАЦІЙНЕ САМОВИЗНАЧЕННЯ МІЖ ЗАКОНОДАВСТВОМ ТА ВПРОВАДЖЕННЯМ

Найлаа Флайїх*, Могаммед Гассон Алі, Агмад Фаділ та Халед Алджасмі

АНОТАЦІЯ

Вступ. *Право на інформаційне самовизначення стало ключовим компонентом цифрових прав в епоху штучного інтелекту та великих обсягів даних. Вкорінене в ширшому праві на приватність, це право дозволяє особам контролювати збір, використання та поширення своїх персональних даних. Незважаючи на його визнання в таких документах, як Загальний регламент про захист даних (GDPR), існує значний розрив між правовою базою та її практичним впровадженням. Метою цього дослідження, що зосереджене на європейському праві, є аналіз розбіжностей між законодавчими гарантіями та реаліями правозастосування. Щораз більша складність цифрових технологій та поява нових категорій даних, таких як ментальні дані, кидають виклик як правовим доктринам, так і інституційним можливостям.*

Методи. *У дослідженні використовується доктринальний правовий аналіз, що спирається на комплексне вивчення положень GDPR, судових прецедентів Суду Європейського Союзу, звітів національних наглядових органів та академічних коментарів. Елементи порівняння застосовані для контекстуалізації європейської системи в межах ширшого міжнародного розвитку. Практичні випадки та моделі нормативно-правового*

забезпечення використовуються для виявлення прогалин та оцінки ефективності чинних механізмів. Дослідження також містить аналітичну оцінку алгоритмічних середовищ та їхнього впливу на згоду, прозорість та індивідуальну діяльність.

Результати та висновки. *Дослідження показує, що хоча GDPR пропонує надійну структуру для захисту персональних даних, його практичному застосуванню перешкоджають структурні, технічні та інтерпретаційні проблеми. Згода часто є неефективною в контекстах, що керуються штучним інтелектом; люди мають труднощі з реалізацією своїх прав, а нормативно-правове забезпечення залишається нерівномірним у різних державах-членах ЄС. У дослідженні увага звертається на необхідність гармонізованої інституційної моделі, вдосконалених інтерфейсів користувача та правового визнання нових типів даних, таких як ментальні дані. Висновок дослідження полягає в тому, що подолання розриву між законодавством та впровадженням вимагає інтеграції правових, технологічних та етичних інструментів у єдину систему, підтверджуючи право на інформаційне самовизначення як наріжний камінь людської гідності в епоху цифровізації.*

Ключові слова: *захист персональних даних, інформаційне самовизначення, права суб'єкта даних, інформаційна конфіденційність, GDPR.*