UDC 347.9
DOI: 10.56215/naia-chasopis/1.2025.48

Legal paternalism's influence on the balancing data protection and fundamental rights

Iurie Patricheev*
Master of Laws
European Court of Human Rights, Council of Europe
67075, 1 de l'Europe Ave., Strasbourg, France
https://orcid.org/0009-0008-5372-4279

Abstract
This article explored how the General Data Protection Regulation, seen as an element of the regime of European regulatory private law, reflects both soft and hard forms of legal paternalism. Employing a doctrinal methodology, this research analysed relevant EU law and the CJEU's jurisprudence in order to examine how the regulation of the right to personal data protection in the European Union's legal order is informed by soft and hard types of legal paternalism. The findings reveal that the General Data Protection Regulation imposes strict obligations on data processors, highlighting a hard paternalistic approach because compliance with such obligations, by implication, limits data subjects' autonomy. Soft paternalism, on the other hand, can be seen in EU lawmakers' attempts to nudge data subjects into using their data carefully and reasonably in digital environments without heavily restricting their data autonomy. This approach raises concerns about the proportionality of restrictions on other fundamental rights, as hard paternalism of the European Union's primary law in this field is strongly reflected in the jurisprudence of the Luxembourg Court that prioritises data protection over competing public interests. A possible way to address this issue is recalibration towards soft paternalism to enhance data subjects' autonomy and improve the balance between privacy and other rights. Such a shift could lead to more context-sensitive rulings emphasising the importance of protection of other human rights

Keywords:
European regulatory private law; European Union; GDPR; EU law; human rights; proportionality; balancing exercise

Introduction

European regulatory private law is a term that academics have coined to explain how the European Union (EU) integrates regulatory objectives within the framework of private law to address public interests and prevent market failures (Cherednychenko, 2021). This analytical approach allows to emphasise the role of private law in achieving regulatory goals, such as consumer protection, financial stability, and fair competition, all of which are underpinned by the EU's origins of an economic organisation (Parsons, 2003). In the context of this article, it is important to highlight the horizontal effect of fundamental rights, where private law is influenced by public law principles, and the interplay between EU market regulation and national private law, which, as M.W. Hesselink (2017) points out, are key elements of the regime. Like any other field of law, it could not escape the changes that the internet revolution brought about (Brownsworth, 2019).

J. Padilla *et al.* (2022) highlight the transformative impact of information technology on human

Article's History:
Received: 01.12.2024
Revised: 25.02.2025
Accepted: 25.03.2025

Suggest Citation:
Patricheev, Iu. (2025). Legal paternalism's influence on the balancing data protection and fundamental rights. *Law Journal of the National Academy of Internal Affairs*, 15(1), 48-58. doi: 10.56215/naia-chasopis/1.2025.48.

*Corresponding author

interactions and data practices in the digital era. With the proliferation of social media and search engines, we increasingly generate more personal data. Numerous tech companies have developed business models that prioritise the collection and use of such data, allowing them to tailor their products and generate profit. However, aside from economic benefits for data processors, these practices raise significant concerns over data protection for data subjects. Given the users' vulnerability to data abuses, it was necessary to regulate this area. In the EU's legal regime, one such piece of legislation is the General Data Protection Regulation (GDPR)[1].

According to S. Khadzhiradieva *et al*. (2024), as a mechanism for the protection of the right to personal data protection guaranteed by the EU Charter of Fundamental Rights[2], the GDPR inextricably pertains to the Union's regime for fundamental rights protection. It makes part of the EU regulatory private law regime, as by its adoption law- and policy-makers intended to influence horizontal private relationships so that they would account for human rights-induced public interests. However, the implementation of this regulation's rights sparked academic debates, particularly regarding their clashes with fundamental rights (used interchangeably with public interests in this article), such as freedom of expression and the right to access information (Veale *et al*., 2018). Taking into account the different approaches of Brussels officials to the regulation of technological progress, as noted by O. Cherednychenko (2024), the issue requires further research.

The purpose of this Article is to examine the extent to which the regulation of the right to personal data protection in European regulatory private law reflects soft and hard forms of legal paternalism and its impact on balancing this right with competing fundamental rights.

Theoretical Framework

Soft and hard legal paternalism in EU law. To embed this article's research question in the academic findings, this section first introduces the concept of legal paternalism. It uses examples from European regulatory private law in the data protection domain to describe two forms of paternalism – soft and hard. Secondly, it elucidates the logic behind the balancing exercise between fundamental rights in EU law. Finally, this section points to a gap in the literature at the intersection of these two academic discussions. Legal paternalism is a legal theory that frames state interference with individuals' decision-making autonomy as justifiable when the latter's unrestricted decisions are reasonably expected to harm themselves (Dworkin, 1972). Developed in the area of law and economics to have an instrumental character (Feinberg, 1971), this concept has been applied to multiple fields of law. Fundamental rights law is no exception, as it also aims at protecting people, overriding their will when necessary (Lixinski & Peleg, 2022). Publicists typically distinguish between two forms of legal paternalism – soft and hard (Ogus, 2010). Nevertheless, one regulation may contain elements of both (Fateh-Moghadam & Gutmann, 2014).

Soft paternalism allows individuals to retain decision-making autonomy while nudging them towards decisions presumed to be in their own interest (Sun, 2024). Thus, instead of imposing strict "command-and-control" rules (Cafaggi & Watt, 2009), this approach mildly influences individuals' decision-making. For instance, the GDPR[3] entitles data subjects to exercise control over their data through rights to consent (Article 6(1)(a) GDPR) and access to personal data (Article 15 GDPR), two cornerstones of data protection (Safari, 2016). Moreover, Articles 13 and 14 develop sophisticated requirements to ensure that data subjects are informed about their data's processing. The inclusion of these safeguards rests on the assumption that individuals might not be aware of the harmful consequences of their data-related choices. Hence, they require more legal protection to avoid reasonably expected harm. To achieve this, EU regulators followed what A. Ogus (2010) viewed as an "ambitious" approach to soft paternalism: they framed the choice "in such a way that more thought and effort is required of the individual before the riskier option can be taken". As data subjects are entitled to be well-informed about the operations relating to their data and have several rights to address their potential maltreatment, they are expected to think twice before opting for riskier digital market options.

On the other hand, hard paternalism mandates protective measures limiting individual freedom of choice to prevent self-harm (Ogus, 2010). Within the EU data protection framework, aspects of hard paternalism restrict data subjects' decision-making autonomy by imposing strict obligations on data processors. Examples include prohibitions on automated decision-making and profiling (Article 22 GDPR) and the obligation to provide data protection by design and by default (Article 25 GDPR). The former exemplifies hard paternalism, as it establishes strict boundaries around data processors' decision-making autonomy, even when data

[1] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[2] Charter of the Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[3] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

subjects might be willing to accept the risks of automated decision-making and profiling in pursuit of personal interests (Solove, 2012).

Similarly, Article 25 GDPR requires processors to ensure personal data protection from the outset of any processing activity. For data subjects, it means that they have to take additional steps, often requiring technological skills, to knowingly opt for weaker protection. Even then, uncompromising minimum standards are non-negotiable, taking away data subjects' autonomy entirely. As these rules prescribe strict conditions (Bygrave, 2017), they leave little leeway for data processors to avoid them. Thus, these examples highlight hard paternalistic logic, as they operate to override the personal preferences of data processors and, by implication, data subjects, in favour of the latter's interests – such as minimising privacy breaches and promoting data security.

From this discussion follows that EU regulators adopted a combined approach to regulating the right to data protection. Its soft paternalistic side entitles data subjects to certain rights. In contrast, in the context of data processors' obligations, they introduced a harder paternalistic element. This regulatory choice attempts to remedy the inherent information asymmetry between data subjects and data processors in digital markets, which makes them prone to market failure. The GDPR's preparatory works show that its drafters were aware of the imbalances between data subjects and data processors and decided to address this situation by imposing more obligations on data processors (European Parliament, 2013). In practice, numerous incidents of data abuses, such as the infamous Facebook-Cambridge Analytica scandal (González-Pizarro *et al*., 2024), evidence the need to regulate this domain to protect data subjects' rights. In this light, guiding consumers towards reasonable handling of their data through legal guarantees (soft paternalism) and imposing mandatory legal obligations on data processors (hard paternalism) is a significant step towards digital market equilibrium.

Balancing competing fundamental rights in the EU legal order. As flows from the above discussion of legal paternalism, one of its key features is balancing the different interests of individuals. EU fundamental rights law shares this approach. For instance, Recital 4 of the GDPR stipulates that the right to data protection is not absolute, implying that it may be legitimately restricted to protect other fundamental rights. Additionally, at the early stages of the Regulation's drafting, EU lawmakers underlined the importance of reconciling data protection rights with public interests to strike "a fair balance of the various [public] interests involved" (European Parliament, 2013). Given the broad scope of the right to data protection (Lynskey, 2023), any attempted restriction should be carefully tailored. Thus, EU regulators prescribed the need to conduct a proportionality test when balancing the right to data protection against competing fundamental rights (Dalla Corte, 2022), and the CJEU's jurisprudence has elaborated on its conditions.

This balancing exercise consists of three key elements[1]. Firstly, it should observe the principle of proportionality that requires any limitation on the right to data protection to be necessary to achieve a legitimate aim without interfering excessively with the rights of data subjects (Zelger, 2022). It is an essential principle of the EU's legal framework (Imamović *et al.*, 2024) which applies universally as a "panacea" for balancing fundamental rights (Justickis, 2020). Secondly, the context of data processing is important, as economic considerations, relevant processing techniques, and the involvement of law enforcement agencies may shift the balance (Kedzior, 2021). Thirdly, the nature of the competing rights comes into play, as in European societies, different human rights require varying degrees of protection (Lenaerts, 2019). The last element was highlighted by the former Organisation of American States' Special Rapporteur for Freedom of Expression, Edison Lanza, who argued that in Europe rights to privacy and data protection historically enjoy more protection compared to the freedom of expression (Organisation of American States, 2017). Finally, it is crucial to consider all three elements of the balancing exercise cumulatively when an authority thinks that it may legitimately limit one's right to data protection.

Nonetheless, despite extensive academic discussions of legal paternalism and the balancing of fundamental rights within EU law, an important topic at the intersection of these fields remains under-researched. Namely, legal scholars have not analysed how different forms of paternalism influence the balancing of fundamental rights in the field of data protection. What remains unexplained is the role that different approaches to legal paternalism can play in addressing conflicts between the digital age rights (under the EU Charter and the GDPR) and public interests, most prominently the right to freedom of expression and the public's right to information.

Materials and Methods

This research employed doctrinal legal methodology, which implies a detailed examination of legislation and related jurisprudence to assess a legal framework governing a particular issue (Bhat, 2019). Following this method, it aimed at exploring the existing EU data protection regulatory framework to identify elements of

[1] Judgment of the European Court of Justice in Case No. C-210/00 "Käserei Champignon Hofmeister GmbH & Co. KG v. Hauptzollamt Hamburg-Jonas". (2002, July). Retrieved from https://curia.europa.eu/juris/showPdf.jsf;jsessionid=2304A21D519F98562C6EC55051260260?text=&docid=47091&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=27753201.

soft and hard paternalism therein and inquired into the extent to which it can effectively address the conflicts between the competing interests of data subjects, data processors, and the general public. This method is particularly suitable for this article's research question, as it provides an opportunity to comprehensively engage with judicial interpretations of relevant legal provisions in order to discern different forms of legal paternalism therein. From a normative perspective, the paternalist assumption that individuals often require protection to minimise self-harm, illuminates regulatory trade-offs between data subjects' decision-making autonomy and protection.

This Article analysed the two most relevant laws in this context – the EU Charter[1] and the GDPR[2]. Their examination was supported by relevant discussions from both laws' *travaux préparatoires*, as these documents can elucidate EU legislators' approach to data protection rights and their relationship with other fundamental rights. Moreover, to construct this thesis, attention is paid to the reasoning from the CJEU's (Court of Justice of the EU) and the ECtHR's (European Court of Human Rights) relevant judgments. This study resorts to the former's jurisprudence given that the Luxembourg Court is the best positioned judicial authority to interpret primary rules of EU law. The Strasbourg Court's case law was used because many of its judgments touch upon human rights whose content is essentially the same as of those protected by the EU regime for fundamental rights protection. The guiding criteria for selecting cases were their relevance and importance for the topic of this research.

Results and Discussion

Internal balancing exercise: Right to personal data protection in the EU. Article 4(1) of GDPR provides more clarity to what is meant by "data" in the EU legal system through an all-encompassing definition (Clarke *et al.*, 2019), codifying it as "any information relating to an identified or identifiable natural person". Article 8(1) of the EU Charter[3] stipulates that "[e]veryone has the right to the protection of [their] personal data". As is often the case in human rights law (Trstenjak, 2023), the following provision of this Article provides more legal certainty by enumerating a list of conditions for lawful data processing. It should be done "fairly", "for specified purposes", and "on the basis of the consent of the person concerned or some other legitimate aims laid down by law" (Article 8(2)). Additionally, the inclusion of adjacent rights, the "right of access" and the "right to have [personal data] rectified" (Article 8(2)), clarifies the scope of this provision. As the subsequent practice of the European Parliament (2018; 2023) suggests, EU lawmakers attempt to ensure that the Union's regime for fundamental rights protection does not lag behind technological developments. Finally, Article 8(3) tasks independent authorities to monitor compliance with the obligations included therein.

Regarding soft paternalism, Article 8 of the EU Charter generally entitles data subjects to the protection of their data. This regulatory approach bears soft paternalist connotations, as it empowers individuals to exercise control over their personal data by facilitating access to data or their rectification. Moreover, the consent and fair processing requirements, developed into self-standing rights under the GDPR (Articles 5(1)(a), 7), ensure that data subjects have control over their data and can make informed decisions about their use. In the case of "Digital Rights Ireland", the CJEU highlighted the importance of making these legal guarantees effective to protect data subjects against potential abuses by data processors[4]. While data subjects might not pay attention to these requirements and decide not to invoke their rights, they cannot "consent away" the minimum protection of these principles (Quelle, 2017). This approach reflects soft paternalism because it aims to mildly influence data subjects' market behaviour by incentivising them to make informed decisions about their personal data without imposing restrictions on the autonomy of their actions.

On the other hand, this rule and its GDPR derivatives impose legal obligations on data processors that, by indirectly limiting data subjects' autonomy, reflect elements of hard paternalism. For instance, one may think of Article 9 on the processing of sensitive data. This provision places data processors under stringent obligations to justify sensitive data processing and to install safeguards against abuses (Quinn & Malgieri, 2021), particularly by demanding a special type of consent. However, it limits data subjects' ability to easily consent to the processing of their sensitive data, which can be problematic in the context of medical and health services or convenience in digital platforms. Although data subjects might want their sensitive data processed swiftly to satisfy personal interests (such as immediate access to healthcare or better digital

[1] Charter of the Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[2] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[3] Charter of the Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[4] Judgment of the European Court of Justice in Joined Cases Nos. C-293/12 & C-594/12 "Digital Rights Ireland Ltd v Minister for Communication, Marine and Natural Resources and Others". (2014, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

services optimisation), strict obligations on data processors from Article 9 preclude this option. In a recent case, the CJEU confirmed the stringent nature of these obligations, requiring a solid legal basis and indicating specific conditions and limits for the processing of sensitive data[1]. The logic of these limitations highlights their hard paternalistic nature, as they aim at protecting data subjects from abuses of personal data and, in doing so, leave no room for manoeuvre for data processors and data subjects.

Unsurprisingly, in relevant cases before the CJEU, such as the Schrems saga, the issue at stake was big companies' unwillingness to grant access to, or delete, personal data because it would compromise their business models[2,3]. Additionally, in "La Quadrature du Net", the CJEU has emphasised that Article 8(2) of the Charter imposes strict obligations concerning the purposes of data processing, meaning that in the absence of the data subject's consent, the processor should put forward a solid legitimate basis for legitimising such processing[4]. The narrow scope of the consent as a legitimate basis for the processing of personal data, which the EU Court interpreted in "Bundeskartellamt", taking the GDPR into account, as "freely given, specific, informed and unambiguous"[5], limits the autonomy of data processors (and data subjects) even more, emphasising Brussels regulators' hard paternalism.

Furthermore, included in the GDPR and recently discussed in the CJEU's "RW v. Österreichische Post AG" judgment[6], requirements of accountability and transparency illustrate the hard paternalism of Article 8. They require data processors to adopt appropriate technical and organisational measures to ensure compliance with the rules on data processing, imposing a higher level of responsibility on them (de Hert & Lazcoz, 2022). As these measures are often costly to develop and implement because they require investments in research and development, the price that consumers pay for data processors' services increases. It is further facilitated by the fact that in modern digital markets, consumers face increasing difficulties in changing their service providers (Kanter, 2023). Hence, it indirectly limits data subjects' decision-making autonomy because financial considerations influence their digital market activities.

Finally, the existence of an independent authority that monitors compliance with Article 8 adds to the restrictions on data processors' autonomy. In multiple decisions, the CJEU considered the existence of such an independent authority a crucial component of the EU data protection regime[7,8,9]. It's very recent verdict in "TR v. Land Hessen" reiterates the importance of granting supervisory authority with effective powers to achieve "control" over the data processors' obligations within the meaning of Article 8(3) of the Charter[10]. As such authorities, operating both at national and EU levels, often fine data processors severely and order them to adjust their business models to comply with Article 8 and the GDPR[11] requirements, it places an additional burden on data processors (Tambou, 2019), which eventually results in more costs (financial and data-related) and fewer features (reduced personalisation and service availability) for consumers.

Therefore, we can conclude that EU regulators' approach to the right to personal data protection combines elements of soft and hard paternalism to address imbalances inherent to digital markets. By granting data subjects freedom of conduct with legal guarantees that aim at shaping their market behaviour (soft paternalism) and imposing mandatory legal obligations on data processors that indirectly shape consumers' decisions (hard paternalism), the EU strives to balance the market inequalities and protect individuals' fundamental right to data protection. In this context, we can see that

[1] Judgment of the European Court of Justice in Case No. C-667/21 "ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des Öffentlichen Rechts". (2023, May). Retrieved from https://eur-lex.europa.eu/leaagal-content/EN/TXT/PDF/?uri=CELEX:62021CA0667.
[2] Judgment of the European Court of Justice in Case No. C-498/16 "Maximilian Schrems v Facebook Ireland Limited". (2018, January). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-498/16.
[3] Judgment of the European Court of Justice in Case No. C-311/18 "Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems". (2020, July). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-311/18.
[4] Judgment of the European Court of Justice in Joined Cases Nos. C-511/18, C-512/18 & C-520/18 "La Quadrature du Net and Others v. Premier Ministre and Others". (2020, October). Retrieved from https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18.
[5] Judgment of the European Court of Justice in Case No. C-252/21 "Meta Platforms Inc, Meta Platforms Ireland Ltd and Facebook Deutschland GmbH v. Bundeskartellamt". (2023, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252.
[6] Judgment of the European Court of Justice in Case No. C-154/21 "RW v. Österreichische Post AG". (2023, January). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0154.
[7] Judgment of the European Court of Justice in Case No. C-518/07 "Commission v. Germany". (2010, March). Retrieved from https://curia.europa.eu/juris/liste.jsf?language=en&num=C-518/07.
[8] Judgment of the European Court of Justice in Case No. C-614/10 "Commission v. Austria". (2012, October). Retrieved from https://curia.europa.eu/juris/document/document.jsf?docid=128563&doclang=EN.
[9] Judgment of the European Court of Justice in Case No. C-288/12 "Commission v. Hungary". (2014, April). Retrieved from https://curia.europa.eu/juris/document/document.jsf?docid=150641&doclang=EN.
[10] Judgment of the European Court of Justice in Case No. C-768/21 "TR v. Land Hessen". (2021, December). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_138_R_0009.
[11] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Brussels regulators' and Luxembourg judges' approach to the implementation of the right to data protection is in itself an "internal" balancing exercise.

However, another important observation is that elements of hard paternalism seem to dominate this approach. The CJEU in numerous decisions interpreted and applied the right to data protection as increasingly imposing restrictions on data processors. By implication, these developments affect data subjects' decision-making autonomy, as they limit the latter's choices in the digital market. With this in mind, this author now proceeds to analyse how this logic informs the broader, "external", balancing exercise between the right to data protection and other fundamental rights.

The role of soft and hard paternalism in the external balancing exercise. This section argues that the internal balancing exercise between soft and hard paternalism in the EU legal framework for personal data protection shapes the external balancing of data protection against competing public interests. Most prominently, those are freedom of expression, access to information, and national security. To this end, the analysis delves deeper into the relevant legal provisions and case law to assess how the internal balancing of paternalism informs the external balancing of fundamental rights.

The CJEU's judgment in "Planet49" is an important starting point in this discussion. There, the Court ruled that pre-ticked[1] checkboxes are not an adequate measure of receiving the data subject's consent under the GDPR. While academics praised this decision as a significant step towards the protection of data subjects (Jabłonowska & Michałowicz, 2020), it can also be read as the CJEU recognising that data subjects are often overwhelmed by the informational overload in digital markets. Hence, we can reasonably argue that the soft paternalist side of the internal balancing exercise might be insufficient to ensure the effective protection of data subjects' right to data protection. Consequently, one may reasonably expect harder paternalist measures against the other side of the digital market to change this situation.

In several other cases[2,3], the CJEU had to address a specific element of the right to data protection, the right to be forgotten, and its relationship with conflicting public interests of freedom of expression and access to information. The right to be forgotten (Article 17 GDPR[4]) entitles data subjects to request the deletion of their personal data if their situation falls under one of the specified conditions (Bunn, 2015). Once the CJEU's decision in Google Spain arrived, it became evident that when the Court emphasises the autonomy of data subjects, it reinforces the dominance of data protection over other fundamental rights. In that case, EU judges prioritised data subjects' right to be forgotten over the public's right to be informed, arguing that when the data in question are excessive or no longer relevant to the aim of processing, the data subject's rights override the competing interests of the data processor and the general public[5].

Five years later, the Court reiterated the correctness of this logic in a related case about the conflict between rights to data protection and to receive information[6]. Furthermore, in "La Quadrature du Net"[7], where the competing interest at stake was that of national security, the CJEU argued that this interest could override the data subject's right to data protection only in specific circumstances, requiring states processing the data in the interests of national security to install an effective system of review of their decisions and limit the duration of data processing. This judicial approach supports the above-mentioned arguments of Special Rapporteur Lanza, according to which the EU data protection regime receives more preferences when compared to other fundamental rights, and prompts several observations.

Firstly, it reinforces numerous academic arguments about the CJEU's inclination towards offering more legal protection to privacy and data protection (Erdos, 2016; Ivanova, 2021). Indeed, when comparing the CJEU's approach to that of the ECtHR[8,9], it becomes clear that the

[1] Judgment of the European Court of Justice in Case No. C-673/17 "Bundesverband der Verbraucherzentralen und Verbraucheverbande–Verbaucherzentrale Bundesverband eV v. Planet49 GmbH". (2019, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0673.

[2] Judgment of the European Court of Justice in Case No. C-136/17 "GC and Others v. Commission Nationale de L'informatique et des Libertés". (2019, September). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-136/17.

[3] Judgment of the European Court of Justice in Case No. C-460/20 "TU and RE v. Google LLC". (2022, December). Retrieved from https://surl.lu/xhyllb.

[4] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[5] Judgment of the European Court of Justice in Case No. C-131/12 "Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González". (2014, May). Retrieved https://curia.europa.eu/juris/liste.jsf?num=C-131/12.

[6] Judgment of the European Court of Justice in Case No. C-507/17 "Google LLC, Successor in Law to Google Inc. v. Commission Nationale de L'informatique et des Libertés (CNIL)". (2019, September). Retrieved from https://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17.

[7] Judgment of the European Court of Justice in Joined Cases Nos. C-511/18, C-512/18 & C-520/18 "La Quadrature du Net and Others v. Premier Ministre and Others". (2020, October). Retrieved from https://surl.li/pirogp.

[8] Judgment of the European Court of Human Rights in Case No. 931/13 "Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland". (2017, June). Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-175121%22]}.

[9] Judgment of the European Court of Human Rights in Cases Nos. 60798/10 & 65599/10 "M.L. and W.W. v. Germany". (2018, June). Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-12041%22]}.

former has a strong preference for data protection. This divergence in approaches can be partly because in the ECtHR's jurisdiction, the right to data protection is not a self-standing right but an element of the right to privacy (Kovalenko, 2022). Even in cases where EU judges acknowledge the possibility that competing fundamental rights may outweigh Article 8 and the GDPR[1] rights, like in "La Quadrature du Net" and "Tele2Sverige and Watson"[2], they prescribe very detailed rules to ensure that limitations of the right to data protection are minimal.

This approach inevitably influences the outcome of the proportionality test, a key element of the external balancing exercise, in favour of the right to data protection. This is particularly so given that the CJEU has interpreted the Union's data protection framework as imposing strict obligations on data processors regarding the aim and conditions of the processing. Additionally, one can find in the CJEU's argumentation references to the context in which data processing takes place, and this context is often employed to advance the data subjects' protection. For instance, in Privacy International, judges indicated the importance of the en masse nature of the data processing in question[3], and this contextual consideration shaped the final ruling which favoured data protection rights. The crucial role that data protection authorities play in the GDPR regime, enforcing data protection legislation, further shifts the balance in favour of the right to data protection[4,5].

Moreover, even the special nature of the competing rights, which shapes the ECtHR's balancing of the right to privacy (when balancing the rights to privacy and freedom of expression, the ECtHR has always reiterated the crucial importance of the freedom of expression for the functioning of democracy[6]), does not affect the EU Court's adamant preference towards the right to data protection. Such a strict approach to all three elements of the external balancing exercise emphasises that hard paternalism within the overall EU data protection framework sets a high bar for any other fundamental rights. The CJEU's message in this respect is, therefore, straightforward – it prioritises data protection unless the opposing public interest is compelling and provides guarantees against abuses.

Secondly, critical concerns should be raised as to whether the external balancing test, dominated by hard paternalism, is capable of accounting for the full range of contemporary public interests. Drawing another analogy with the ECtHR, the Strasbourg provision that encompasses the right to data protection acknowledges the following list of legitimate aims: "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"[7]. It is much longer than the number of accepted by the CJEU public interests.

Earlier drafts of Article 8 of the EU Charter were initially cautious about confrontations with other legitimate interests. As such, the very first version included a safeguard that the right to data protection should not "conflict with the rights of third persons" (Coghlan & Steiert, 2021). It also provided that "[r]estrictions shall be admissible by law only in the dominant general interest" (Coghlan & Steiert, 2021). Later on, amendments to define the scope of "the dominant general interest" and to incorporate the principle of proportionality were successfully adopted (Coghlan & Steiert, 2021). The final wording of Article 8 indicates that the list of legitimate bases to be invoked for data processing is non-exhaustive: "[...] or some other legitimate basis laid down by law".

Taken together with Recital 40 of the GDPR, it means that domestic legislators are, in principle, free to prescribe legal bases for the lawful processing of personal data. It will then be EU judges' task to decide whether these bases represent legitimate aims for restricting one's data protection rights. So far, the CJEU has acknowledged that public interests of being informed and national security may justify interference with the right to data protection. It also recognised the economic interests of data processors. However, the Court imposed stringent safeguards against potential data abuses, leading to the conclusion that sophisticated data protection should be the norm and derogations – the exception.

This approach is structurally rigid, as in the external balancing exercise data protection seems to occupy a paramount position, leaving little room for

[1] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[2] Judgment of the European Court of Justice in Joined Cases Nos. C-203/15 and C-698/15 "Tele2Sverige AB v. Post-och Telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis". (2016, December). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-203/15.

[3] Judgment of the European Court of Justice in Case No. C-623/17 "Reference for a Preliminary Ruling from the Investigatory Powers Tribunal – London (United Kingdom) Made on 31 October 2017 – Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others". (2020, October). Retrieved from https://surl.li/hnbvxm.

[4] Judgment of the European Court of Justice in Case No. C-210/16 "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH". (2018, June). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-210/16.

[5] Judgment of the European Court of Justice in Case No. C-311/18 "Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems". (2020, July). Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

[6] Judgment of the European Court of Human Rights in Case No. 25344/20 & 17 others "Friedrich and Others v. Poland". (2024, June). Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-234267%22]}.

[7] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://surl.li/cetvkq.

other fundamental rights to be successfully weighed against it. Moreover, it is difficult to reconcile with the above discussion of the evolution of the right to data protection in the EU Charter's preparatory works and raises questions regarding the role that the principle of fairness plays in EU data protection law (Clifford & Ausloos, 2018). The main reason is that the internal balancing exercise's hard paternalism, which the CJEU subsequently developed to apply to the external balancing exercise, led to very strict scrutiny of any public interest that data processors might advance to justify the processing of personal data.

Conclusions

This Article highlighted that the EU's data protection regulatory framework strikes a balance between hard and soft forms of legal paternalism. In this light, the GDPR safeguards individual fundamental rights in digital environments and establishes a legal regime that compensates for the inherent power imbalances between data subjects and data processors. One can notice the prevalence of hard paternalism in this approach, as the Regulation imposes strict obligations on data processors which indirectly curb data subjects' autonomy. This leads to a situation where data subjects, as consumers in digital markets, are deprived of choices that they would otherwise want to take, either financially or quantitatively.

This inflexible paternalistic approach broaches critical questions about the future of the EU human rights law in the digital age. If Brussels' hard paternalistic policy spills over other regulatory domains where personal data play a role (financial regulation or electronic communications), the risk of solidifying data protection as an almost untouchable right raises concerns about the proportionality of restrictions on other fundamental rights. It has already become visible in the CJEU's strong preference towards the right to data protection, with the external balancing exercise taking high data protection standards almost as a default setting. In these circumstances, data processors struggle to have their potentially legitimate interests accepted to restrict data subjects' rights. It raises serious concerns about a potential hierarchy of EU fundamental rights, which would be difficult to reconcile with the mainstream approach of international human rights law that upholds the equal importance of different fundamental rights.

A practical recalibration towards soft paternalism could offer a solution. This recalibration would involve enhancing the autonomy of data subjects by refining information requirements and consent mechanisms. With more efficient techniques tailored to avoid information overload, data subjects will be able to make more informed choices about how their data are used. Additionally, with more granular options for consent, they could better balance their desire for privacy against competing interests. It would foster greater flexibility, allowing individuals to pursue their preferences without being confined to rigid protections.

In such an arrangement, soft paternalism would also play a more prominent role in the external balancing equation, allowing for a better degree of proportionality there. By efficiently "educating" data subjects and allowing them to exercise more control over their data, regulators could move away from imposing hard paternalistic measures as a default. This would open space for more context-sensitive rulings where judges could weigh other fundamental rights more equitably against privacy concerns. However, as the interpretation and application of the GDPR are technical legal matters, such a change should originate in the Luxembourg court.

Further research may explore how to institutionalise this shift in the EU's legal framework. One particular suggestion is a comparative analysis of the CJEU's and the ECtHR's approaches to balancing the right to data protection with competing fundamental rights. Such research, especially considering the EU's aspirations to accede to the ECHR, may indicate alternative options to incorporate the full spectrum of modern European public interests in the external balancing exercise without compromising the robustness of the EU data protection regime.

Acknowledgements

The author would like to thank Professor Olha Cherednychenko, Eva Rippe, and Sina Platzbecker for their comments on the earlier drafts of this article.

Conflict of Interest

The author of this study declares no conflict of interest. This research was conducted in the course of the author's postgraduate studies and does not represent the views of his current employer.

References

[1] Bhat, P.I. (2019). *Doctrinal legal research as a means of synthesizing facts, thoughts, and legal principles.* Oxford: Oxford University Press. doi: 10.1093/oso/9780199493098.003.0005.

[2] Brownsworth, R. (2019). Legal rules, technological disruption, and legal/regulatory mindsets. In R. Brownsworth (Ed.), *Law, technology and society: Reimagining the regulatory environment* (pp. 181-204). New York: Routledge. doi: 10.4324/9781351128186.

[3] Bunn, A. (2015). The curious case of the right to be forgotten. *Computer Law & Security Review*, 31(3), 336-350. doi: 10.1016/j.clsr.2015.03.006.

[4] Bygrave, L.A. (2017). Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review*, 4(2), 105-120. doi: 10.18261/issn.2387-3299-2017-02-03.
[5] Cafaggi, F., & Watt, H.M. (2009). *The regulatory function of European private law.* Edward London: Elgar Publishing. doi: 10.1017/9781108565417.036.
[6] Cherednychenko, O. (2021). Islands and the ocean: Three models of the relationship between EU market regulation and national private law. *Modern Law Review*, 84(6), 1294-1329. doi: 10.1111/1468-2230.12664.
[7] Cherednychenko, O. (2024). EU Financial regulation and private law: Towards a holistic approach. In M. Heidemann (Ed.), *The transformation of private law – principles of contract and tort as European and international law* (pp. 855-882). Cham: Springer. doi: 10.1007/978-3-031-28497-7_39.
[8] Clarke, N., Vale, G., Reeves, E.P., Kirwan, M., Smith, D., Farrell, M., Hurl, G., & McElvaney, N.G. (2019). GDPR: An impediment to research? *Irish Journal of Medical Science*, 188(1), 1129-1135. doi: 10.1007/s11845-019-01980-2.
[9] Clifford, D., & Ausloos, J. (2018). Data protection and the role of fairness. *Yearbook of European Law*, 37(1), 130-187. doi: 10.1093/yel/yey004.
[10] Coghlan, N., & Steiert, M. (2021). *The Charter of Fundamental Rights of the European Union: The travaux préparatoires and selected documents.* Florence: European University Institute Publishing. doi: 10.2870/004119.
[11] Dalla Corte, L. (2022). On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, 12(4), 259-275. doi: 10.1093/idpl/ipac014.
[12] De Hert, P., & Lazcoz, G. (2022). When GDPR-principles blind each other: Accountability, not transparency, at the heart of algorithmic governance. *European Data Protection Law Review*, 8(1), 31-40. doi: 10.21552/edpl/2022/1/7.
[13] Dworkin, G. (1972). Paternalism. *Philosophy and Public Policy,* 56(1), 64-75. doi: 10.1017/S026626710000359X.
[14] Erdos, D. (2016). European union data protection law and media expression: Fundamentally off balance. *European Comparative Law Quarterly*, 65(1), 139-183. doi: 10.1017/S0020589315000512.
[15] European Parliament. (2013). *Report on the proposal for a regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data (General Data Protection Regulation) (COM(2012)0011–C7-0025/2012–2012/0011(COD))*. Retrieved from https://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf.
[16] European Parliament. (2018). *Recording of the Plenary Session of 23/10/2018*. Retrieved from https://multimedia.europarl.europa.eu/en/webstreaming/plenary_20181023-0900-PLENARY?seekTo=181023090224.
[17] European Parliament. (2023). *Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US data privacy framework (2023/2501(RSP))*. Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html.
[18] Fateh-Moghadam, B., & Gutmann, T. (2014). Governing [through] autonomy. The moral and legal limits of "soft paternalism". *Ethical Theory and Moral Practice*, 17(3), 383-397. doi: 10.1007/s10677-013-9450-3.
[19] Feinberg, J. (1971). Legal paternalism. *Canadian Journal of Philosophy*, 1(1), 105-124. doi: 10.1080/00455091.1971.10716012.
[20] González-Pizarro, F., Figueroa, A., López, C., & Aragon, C. (2022). Regional differences in information privacy concerns after the Facebook-Cambridge Analytica data scandal. *ECSCW Contributions*, 31(1), 33-77. doi: 10.1007/s10606-021-09422-3.
[21] Hesselink, M.W. (2017). Private law, regulation, and justice. *European Law Journal*, 22(5), 681-695. doi: 10.1111/eulj.12195.
[22] Imamović, S., Börjedal, E., & Di Franco, E. (2024). The future of EU fundamental rights. *Maastricht Journal of European and Comparative Law*, 31(2), 137-146. doi: 10.1177/1023263X241290470.
[23] Ivanova, Y. (2021). The role of EU fundamental right to data protection in an algorithmic and big data world. In D. Hallinan, R. Leenes, S. Gutwirth & P. De Hert (Eds.), *Data protection and privacy, volume 13: Data protection and artificial intelligence*. New York: Bloomsbury Publishing. doi: 10.2139/ssrn.3697089.
[24] Jabłonowska, A., & Michałowicz, A. (2020). Planet49: Pre-ticked checkboxes are not sufficient to convey user's consent to the storage of cookies (C-673/17 Planet49). *European Data Protection Law Review*, 6(1), 137-142. doi: 10.21552/edpl/2020/1/19.
[25] Justickis, V. (2020). Balancing personal data protection with other human rights and public interest: Between theory and practice. *Baltic Journal of Law and Politics*, 13(1), 140-162. doi: 10.2478/bjlp-2020-0006.

[26] Kanter, J.S. (2023). Digital markets and "trends towards concentration". *Journal of Antitrust Enforcement*, 11(2), 143-148. doi: 10.1093/jaenfo/jnad030.
[27] Kedzior, M. (2021). The right to data protection and the COVID-19 pandemic: The European approach. *ERA Forum*, 21(4), 533-543. doi: 10.1007/s12027-020-00644-4.
[28] Khadzhiradieva, S., Bezverkhniuk, T., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social and Legal Studios*, 7(3), 245-256. doi: 10.32518/sals3.2024.245.
[29] Kovalenko, Y. (2022). The right to privacy and protection of personal data: Emerging trends and implications for development in jurisprudence of European Court of Human Rights. *Masaryk University Journal of Law and Technology*, 16(1), 37-57. doi: 10.5817/MUJLT2022-1-2.
[30] Lenaerts, K. (2019). Limits on limitations: The essence of fundamental rights in the EU. *German Law Journal*, 20(6), 779-793. doi: 10.1017/glj.2019.62.
[31] Lixinski, L., & Peleg, N. (2022). Paternalism in international human rights law. *Duke Journal of Comparative and International Law*, 33(1), 1-43. doi: 10.2139/ssrn.4342084.
[32] Lynskey, O. (2023). Complete and effective data protection. *Current Legal Problems*, 76(1), 297-344. doi: 10.1093/clp/cuad009.
[33] Ogus, A. (2010). The paradoxes of legal paternalism and how to resolve them. *Legal Studies*, 30(1), 61-73. doi: 10.1111/j.1748-121X.2009.00146.x.
[34] Organisation of American States. (2017). *Annual report of the Office of Special Rapporteur for Freedom of Expression*. Retrieved from https://www.oas.org/en/iachr/expression/reports/annual.asp.
[35] Padilla, J., Piccolo, S., & Vasconcelos, H. (2022). Business models, consumer data and privacy in platform markets. *Journal of Industrial and Business Economics*, 49(3), 599-634. doi: 10.1007/s40812-022-00218-0.
[36] Parsons, C. (2003). Showing ideas as causes: The origins of the European Union. *International Organisation*, 56(1), 47-84. doi: 10.1162/002081802753485133.
[37] Quelle, C. (2017). Not just user control in the General Data Protection Regulation: On the problems with choice and paternalism, and on the point of data protection. In A. Lehmann, D. Whitehouse, S. Fischer-Hübner, L. Fritsch & C. Raab (Eds.), *Privacy and identity management: Facing up to next steps*. New York: Springer. doi: 10.1007/978-3-319-55783-0_11.
[38] Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data – the concept of sensitive data in the EU data protection framework. *German Law Journal*, 22(8), 1583-1612. doi: 10.1017/glj.2021.79.
[39] Safari, B. A. (2016). Intangible privacy rights: How Europe's GDPR will set a new global standard for personal data protection. *Seton Hall Law Review*, 47, 809-848.
[40] Solove, D.J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.
[41] Sun, Y. (2024). Research on legal protection of minor females from the perspective of soft paternalism. *Scientific and Social Research*, 6(1), 154-160. doi: 10.26689/ssr.v6i1.6018.
[42] Tambou, O. (2019). Lessons from the first post-GDPR fines of the CNIL against Google LLC. *European Data Protection Law Review*, 5(1), 80-99. doi: 10.21552/edpl/2019/1/13.
[43] Trstenjak, V. (2023). Limitations of fundamental rights in EU law: Are human rights absolute? *European Review*, 32(2), 135-149. doi: 10.1017/S1062798723000509.
[44] Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, 8(2), 105-123. doi: 10.1093/idpl/ipy002.
[45] Zelger, B. (2023). The right to be forgotten in the European Union: Towards a uniform approach? *Global Privacy Law Review*, 3(1), 19-28. doi: 10.54648/gplr2022003.

Вплив правового патерналізму на баланс між захистом даних і фундаментальними правами

Юрій Патрікеєв
Магістр права
Європейський суд з прав людини, Рада Європи
67075, пр-т. Європа, м. Страсбург, Французька Республіка
https://orcid.org/0009-0008-5372-4279

Анотація
У цій статті досліджено, як Загальний регламент про захист даних, що є елементом режиму європейського регуляторного приватного права, відображає м'які й жорсткі форми правового патерналізму. На основі використання доктринальної методології в цьому дослідженні проаналізовано відповідне право ЄС і практику Суду Європейського Союзу з метою вивчення того, як регулювання права на захист персональних даних у правопорядку ЄС ґрунтується на м'якому та жорсткому типах правового патерналізму. Результати засвідчують, що Загальний регламент про захист даних накладає суворі зобов'язання на обробників даних у межах жорсткого патерналістського підходу, оскільки дотримання таких зобов'язань обмежує автономію суб'єктів даних. М'який патерналізм, з іншого боку, наявний у спробах законодавців ЄС підштовхнути суб'єктів до обережного й розумного використання їхніх даних у цифровому середовищі без значного обмеження їхньої автономії даних. Цей підхід викликає занепокоєння щодо пропорційності обмежень інших основоположних прав, оскільки жорсткий патерналізм основного закону ЄС у цій сфері яскраво відображено в судовій практиці Люксембурзького суду, який надає пріоритет захисту даних над суспільними інтересами, що конкурують. Можливим способом розв'язання цієї проблеми є рекалібрування в напрямі м'якого патерналізму для посилення автономії суб'єктів даних і підтримання балансу між приватним життям й іншими правами. Таке зміщення може призвести до прийняття контекстно чутливіших рішень, що засвідчують важливість захисту інших прав людини

Ключові слова:
європейське регуляторне приватне право; Європейський Союз; GDPR; право ЄС; права людини; пропорційність; балансування