Balancing Privacy and Data Protection: An Introductory Look at Conflicting Constitutional Interests

Giovanni De Gregorio* **and Oreste Pollicino°**

Abstract

The question of privacy and data protection has become a pivotal concern for those examining the long-term sustainability of European digital policies. Balancing privacy and data protection as fundamental rights presents not only theoretical challenges but also practical implications that shape the interpretation and enforcement of digital policies. The European Charter of Fundamental Rights and the European Convention on Human Rights establish a general limitation to the protection of fundamental rights, thus requiring a delicate balancing act among various constitutional interests to safeguard the essence of these rights. Even if the meeting of privacy and data protection with other constitutional rights cannot be addressed by adopting an absolute approach, this constitutional framework has not pre-empted European institutions from extending the scope of privacy and data protection. This paper introduces the analysis of three cases underlining the relevance of proportionality in the conflicts between privacy and data protection and other constitutional interests in the digital age. Then, the paper addresses the challenges raised by the tendency towards enforcing, and protecting, privacy and data protection without carefully balancing the protection of these fundamental rights with other rights and freedoms in Europe.

1. Introduction

The constitutional question around the scope of privacy and data protection in Europe has primarily captured the attention of who is looking at the sustainability of European digital policies in the long run. Indeed, the balancing of privacy and data protection as fundamental rights is not only a theoretical challenge but also leads to practical implications which inevitably shape the interpretation and enforcement of different policy areas in the digital age.

* PLMJ Chair in Law and Technology, Católica Global School of Law, Lisbon.
° Full Professor of Constitutional Law, Bocconi University.

Within the European constitutional framework, the European Charter of Fundamental Rights (Charter) provides a first and primary point of reference. Similarly to the European Convention on Human Rights (Convention),[1] the Charter establishes a general limitation to the protection of fundamental rights and requires balancing different constitutional interests to protect the essence of fundamental rights.[2] This approach is also confirmed by different areas of EU policy which are based on the aim to achieve multiple objectives through the balancing of different constitutional rights, including the respect for private and family life,[3] and a right to the protection of personal data.[4]

Even if this constitutional framework has not pre-empted the CJEU from protecting privacy and personal data extensively, as underlined particularly in the case law on data protection such as *Google Spain*,[5] and *Meta Platforms*,[6] nonetheless, this approach does not automatically grant absolute protection to privacy and data protection in Europe. Other decisions have underlined how privacy and data protection enter into a process of balancing with other constitutional interests, including economic freedoms, as underlined in *Volker*.[7]

If it is not possible to exclude that the European constitutional system is based on a firm dignitary value,[8] the balancing of individual rights and economic freedoms needs to consider the limit of absolute protection which, in the European constitutional framework finds its limit in the clause of abuse of rights. Indeed, despite some differences, both the Convention and the Charter recognise that the protection of rights and freedoms should not lead to interfering with the essence of other constitutional rights in the European framework.[9]

Within this framework, this paper introduces the research conducted by Mikolaj Barzcentewicz, Joan Barata and Raffaele Torino,[10] underlining how the encounter

[1] European Convention on Human Rights (1950), Art. 8.
[2] European Charter of Fundamental Rights (2012), Art. 52.
[3] Ibid, Art. 7.
[4] Ibid, Art. 8.
[5] Case C-131/12, Google Spain (2014). See Oreste Pollicino, *Judicial Protection of Fundamental Rights Online. A Road towards Digital Constitutionalism?* (Hart 2022).
[6] Case C-252/21, Meta Platforms (2023).
[7] Joined cases C-92/09 and C-93/09, Volker (2010).
[8] Catherine Duprè, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Hart 2015).
[9] Convention, Art. 17; Charter, Art. 54.
[10] Joan Barata, 'Freedom of Expression and Privacy on Social Media: the Blurred Line Between the Private and the Public Sphere' MediaLaws (1 August 2023) <https://www.medialaws.eu/freedom-of-expression-and-privacy-on-social-media-the-blurred-line-between-the-private-and-the-public-

between privacy and data protection and other constitutional rights cannot be addressed by adopting an absolute approach, but requires conducting a fair balance between conflicting interests. The lack of balancing is also the result of the tendency towards expanding the scope of privacy and data protection without considering the protection of conflicting constitutional interests in the digital age. In the first part, this paper looks at three cases, precisely those concerning the interoperability mandate in the Digital Markets Act,[11] content moderation and the right to be forgotten, and economic freedoms, primarily freedom to conduct business. The second part briefly looks at the questions raised by the extensive enforcement of privacy and data protection for European digital policies.

2. Balancing Privacy and Data Protection in European Digital Policies

The conflicting relationship of privacy and data protection with other constitutional rights in the digital age does not define a new dynamic. The spread of digital products and services has not only led to opportunities and risks for these fundamental rights but has also amplified the clash between conflicting rights and freedoms. Even if the EU has reacted to this trend, as shown by the adoption of the GDPR,[12] this approach has not solved this constitutional tension which is primarily connected to the balancing between conflicting rights and freedoms in constitutional democracies.

The introduction of the Digital Markets Act has unveiled this clash. Apparently, the Digital Markets Act primarily interferes with economic freedoms in the EU to ensure competition in the internal market. Nonetheless, serious concerns for privacy and data protection also come from this legal instrument. Particularly, the interoperability mandate might produce negative consequences for the protection of privacy and personal data by limiting the possibility for gatekeepers to deal with malicious behaviours.

---

sphere/>.; Mikołaj Barczentewicz, 'Interpreting the EU Digital Markets Act consistently with the EU Charter's rights to privacy and protection of personal data' MediaLaws (3 August 2023) <https://www.medialaws.eu/interpreting-the-eu-digital-markets-act-consistently-with-the-eu-charters-rights-to-privacy-and-protection-of-personal-data/>; Raffaele Torino, 'Freedom to Conduct a Business and Right to the Protection of Personal Data' MediaLaws (4 August 2023) <https://www.medialaws.eu/freedom-to-conduct-a-business-and-right-to-the-protection-of-personal-data/>.

[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828; 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.

According to the Digital Markets Act,[13] gatekeepers cannot prevent users, 'technically or otherwise', from switching between and subscribing to software and services 'accessed using the core platform services of the gatekeeper'. These provisions would limit the possibility for gatekeepers to protecting users' from harmful online behaviours (e.g. phishing), also considering the lack of safeguards to counterbalance the interference with privacy and data protection safeguards. This approach extends to different areas of providers covered by the Digital Markets Act, including messaging services. Therefore, opening the use of multiple services without giving the possibility to restrict access to users to certain dangerous services could not only dilute the purpose of ensuring security but also affects privacy and data protection as fundamental rights.

This approach underlines the constitutional questions raised by privacy and data protection. As underlined by Barczentewicz,[14] calling the role of the Charter leads to balancing between the need to ensure internal market goals and users' protection of fundamental rights. The DMA does not even address in its Recital the role of privacy and data protection as fundamental rights within its structure. Even if the DMA refers to the GDPR,[15] many of the questions raised by the interoperability mandate do not only concern the processing of personal data but also users' privacy and security. Besides, the DMA has introduced a demanding standard of interoperability, for instance, by requiring that any third-party service must offer the same level of security of the original one. As such, this approach to interoperability could affect not only users in terms of privacy and data protection, but also the freedom to conduct business of providers which are the addressees of this mandate.

The questions related to the balancing of privacy and data protection in the European framework have been particularly underlined by content moderation and by the cases related to the right to be forgotten. The role and discretion of online platforms in making decisions on the balancing of privacy and data protection is also a relevant challenge even within the framework of the Digital Services Act.[16]

Already in *Google Spain,* the CJEU extended (or adapted) the scope of fundamental rights in the digital age, thus recognising the obligation for search engines to delist

[13] Digital Markets Act, Art. 6(6).
[14] Barczentewicz (n 10).
[15] Ibid, Art. 8.
[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

personal data from their search results. As underlined by Barata,[17] the CJEU did not focus on the context, primarily the role of search engines in that case, to support its legal reasoning on the right to be forgotten online. This case underlines how the lack of balancing privacy and data protection with other constitutional interests leads to disproportionate effects on freedom of expression, and, particularly, freedom to conduct business considering the privatisation of the enforcement of these rights which emerges in connection, among others, to content moderation activities and the right to be forgotten.

However, the role of balancing has also been underlined in *Google v CNIL*.[18] The CJEU highlighted the different approaches to the right to privacy and data protection in other legal systems as well as the relative nature of this fundamental right. Even if, considering the extensive approach to the protection of privacy and personal data, the coherent solution would have been to extend the right to be forgotten on a global scale, the CJEU opted for a self-restraining approach, motivated by the desire to mitigate the risk of a kind of European legal colonisation in the name of cultural hegemony. The CJEU has followed a similar approach in relation to freedom of expression. Specifically, in *Glawischnig-Piesczek v Facebook*,[19] the CJEU addressed the territorial scope of national orders concerning the removal of content, thus underlining the potential and limited extension of EU law, especially freedom of expression, on a global scale.

These cases underline how the relationship between rights and freedoms is articulated in the digital age. On the one hand, data are critical for the development of the internal market. On the other hand, they also raise constitutional questions about how to protect privacy and data protection as individual fundamental rights and democratic values. Even if the GDPR has driven a new shift in the constitutional approach of the Union to privacy and data protection, it still maintains the core of internal market goals which had already driven the adoption of the Data Protection Directive.[20]

[17] Barata (n 10).
[18] Case C-507/17, Google v. CNIL (2019).
[19] Case C-18/18, Glawischnig-Piesczek v Facebook (2019).
[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The general principles of the GDPR, and primarily accountability,[21] tend to underline the need for data controllers to balance conflicting constitutional interests, particularly in order to ensure the protection of data subjects' rights. As a result, the obligations of data controllers are not always determined by the GDPR but their content is primarily shaped by the context. This approach makes the principle of proportionality the core of European data protection law which drives the balancing among fundamental rights, including economic freedoms.

Furthermore, as underlined by Torino,[22] other areas of EU law confirm the limited scope of privacy and data protection as fundamental rights in the European constitutional framework. The CJEU has considered labour rights, for instance, in *Alemo-Herron,*[23] and intellectual property, such as in *Scarlet,*[24] with privacy and data protection, thus underlining in practice the centrality of balancing constitutional interest. As a result, the predominance of privacy and data protection is not only challenged when it comes to the balancing with other individual rights such as freedom of expression but also with economic interests such as freedom to conduct business.

These cases underline how the protection of privacy and personal data clashes with other rights and freedoms which are also protected in the European constitutional framework. Therefore, proportionality is the core of this system to limit trends towards absolute protection of rights and freedoms, which could overwhelm the other constitutional interests. This framework is also confirmed by the GDPR which introduces the principle of accountability as a way to increase the responsibility of data controllers while leaving spaces to decide the organisation of their compliance system. Nonetheless, when looking at the enforcement of the right to privacy and data protection, the European approach has not always looked at proportionality as guidance for solving constitutional conflicts.

3. Interpreting Privacy and Data Protection in the Digital Age

The protection of privacy and personal data in the digital age has not always been treated as a question of balancing but, rather, as a question of axiology. As primarily underlined in *Google Spain*, this process still characterises the European approach,

[21] GDPR, Art. 5.
[22] Torino (n 10).
[23] Case C-426/11, Alemo-Herron (2013).
[24] Case C-70/10, Scarlet (2010).

even after the adoption of the GDPR which has reinforced the protection of privacy and personal data in Europe. Although the EU has complemented its data policy with the adoption of regulatory instruments, including the Data Governance Act and the Data Act,[25] which underline the market dimension of data, the enforcement of privacy and data protection underlines how these fundamental rights tend to prevail over other conflicting constitutional interests.

The questions around the legal bases to process personal data by online platforms is a primary example of the constitutional challenges raised by digital services in the internal market. In December 2022, the Irish Data Protection Commission imposed a 390€ million fine against Meta for the processing of its users' data for the purposes of targeted advertising based on contractual necessity as legal basis.[26] Nonetheless, this decision was not aimed to react or punish Meta for violating the GDPR, but primarily resulted from the binding opinion of the European Data Protection Board (EDPB) of the same month.[27]

Likewise, in *Meta Platforms*, the Court left little space to rely on alternative legal bases to consent to process personal data for the purposes of targeted advertising. By adopting a strict interpretation, the Court limited the use of legitimate interest and contractual necessity as legal bases in this case, thus emphasising the role of consent. Nonetheless, the Court opened up the possibility for alternatives. According to the Court, users can refuse consent for unnecessary data processing, such as targeted advertising, as long as an equivalent alternative is offered along with adequate compensation. The Court supported the introduction of subscription models as an alternative to targeted advertising. This approach could help to reduce legal uncertainty about the implications for services based on targeted advertising, thus striking a fairer balance between freedom and rights which is at the core of European constitutionalism.

Despite the critical importance of consent as legal basis, this decision appears to underestimate the challenges coming from its outcome. Particularly, the CJEU

[25] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724; Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data COM(2022) 68 final.
[26] Irish Data Protection Commission (31 December 2022).
[27] EDPB, Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) (5 December 2022) <https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf>.

provided the image of a data subject who can express a valid consent, even when accessing the services of a business abusing its dominant position. This approach could lead to considering consent as a formal exercise, thus affecting the rights of data subjects, the very party that is meant to be protected. Furthermore, as in *Google Spain*, the Court did not take into account the implications of this decision, particularly on other digital services that rely on targeted advertising. Although the CJEU acknowledged the significance of personal data access and exploitation in the digital economy, it assigned less importance to these services in the current case, particularly recognising that legitimate interest and contractual necessity cannot be considered as legal bases to process personal data for the purposes of targeted advertising.

In a way, within the European data protection system, the CJEU indirectly recognised the axiological value of consent in ensuring greater protection for data subjects in the digital age, similarly to other approaches followed by other European institutions. The GDPR does not explicitly establish such a hierarchy, but there is a trend towards considering some legal bases, such as consent, as more solid than others like legitimate interest. As a result, contractual necessity and legitimate interest cannot be considered legal bases to process users' data for purposes of targeted advertising. This case provides another example of the unsolved pitfalls of European data protection, from specific questions, including the relationship between legal bases to process personal data, to general concerns about the role of data protection in the internal market.

This approach leads to a conflict with the architecture of the GDPR, particularly the principle of accountability. The GDPR has already required data controllers to adapt their compliance not to a rigid structure but to an evolving process based on a context-based risk assessment. According to the GDPR, it is for data controllers to demonstrate that they have implemented appropriate safeguards to respect the general principles of the GDPR, including lawfulness, and, therefore, the adequate legal basis to protect users' rights. As a result, these decisions restrict the space for the principle of accountability, thus also unexpectedly shaping the role of data controllers when it comes to the processing of personal data in the case of targeted advertising. This situation raises concerns for the possibility of data controllers in the EU to invest resources for complying with the dynamic requirements of the GDPR.

However, the structure of the GDPR provides a guidance to overcoming this situation. Indeed, on the one hand, the GDPR has led to an important step further in

the protection of data subjects' fundamental rights. On the other hand, it still tends to protect economic freedoms in the internal market. This constitutional conflict leads to looking at the principle of accountability as a potential way to limit potential abuses of individual rights or economic freedoms. Therefore, if the principle of accountability helps to strike a balance among constitutional conflicting interests, the primary point is also how to ensure that this principle guides the relationship between national competent authorities and European institutions. The inconsistent enforcement of the GDPR does not only lead to unpredictable sanctions but also undermines the trust and collaboration between public and private actors in determining compliance with the GDPR.

4. Conclusions

The risk of following an absolute approach towards privacy and data protection could lead to a restrictive approach, thus neglecting the central role of balancing in European constitutionalism. The primary challenge is thus that of finding a balance where the protection of individual rights does not translate into a compression of other constitutional interests, including economic freedoms. In other words, it is essential that privacy and data protection are not turned into absolute rights, capable of quashing any other fundamental rights as protected amongst others by the Charter itself and recognised by the GDPR. The mistake for Europe would be to grant absolute protection to privacy and data protection that does not leave space for flexibility to address the transformations of the digital age.

Within the European landscape, the GDPR sets a legal framework which is highly protective of data privacy and data protection rights of individuals across Europe. The GDPR already provides for a range of duties and obligations and provides data subject rights aiming at making data controllers accountable for the data processing activities they put in place and at mitigating the risks connected to them. A disproportionate interpretation of these rules would lead to disregards the accountability framework set out in the GDPR and affect European digital policy.

It is against this backdrop that the principle of proportionality, interpreted as the guiding parameter of European constitutionalism, comes to play a critical role. Proportionality is a key requirement and criterion of legitimacy of any intervention aiming at imposing restrictions upon a fundamental right. This approach has also been reflected within the EU regulatory framework as shown by the increasing resort to so-called "risk-based regulation", whereby risk assessment becomes the proxy to defining the correct degree of duties and obligations to be imposed on market actors,

thus providing another example of the role of proportionality in the digital age. When dealing with a conflict between opposing fundamental rights, the role of proportionality is critical to ensure that none of those rights is subjected to excessive compression.