CATÓLICA Global School of Law

CATÓLICA RESEARCH CENTRE FOR THE FUTURE OF LAW
LISBOA · PORTO

CGSL WORKING PAPERS

No. 3/2024

The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe

Giovanni De Gregorio

Simona Demková

The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe*

Giovanni De Gregorio† *& Simona Demková*‡

Abstract

The consolidation of the digital age has expanded the demand for justice. The challenges characterising digital relationships have led European policy makers to wonder about the opportunity to introduce new safeguards to ensure the right to effective remedies as enshrined in the EU Charter of Fundamental Rights. On the one hand, this approach has triggered the proliferation of new procedures, thus expanding potential remedies. On the other hand, the introduction of new remedies increases fragmentation and uncertainty about their access and functioning. This work examines the challenges for the right to an effective remedy raised by the proliferation of intertwined remedies in three key pieces of European digital regulation – the General Data Protection Regulation, the Digital Services Act, and the Artificial Intelligence Act. Particularly, we assess the three key avenues for remedies, namely internal complaints, independent supervision and judicial remedies. Based on this assessment, we underline the need for further clarity in the interplay between the remedial designs, central to which will be the focus on institutional collaboration across the emerging remedial frameworks.

* Forthcoming (2024) in van Oirsouw, Ch., de Poorter, J.; Leijten, I.; van der Schyff, G.; Stremler, M.; de Visser, M. (eds), *European Yearbook of Constitutional Law*.

† PLMJ Chair in Law and Technology at Católica Global School of Law and Católica Lisbon School of Law.

‡ Assistant Professor of European Law, Leiden University, Europa Institute.

1. Introduction

The digital age has brought new, and amplified the existing, challenges and harms. The demand for justice and effective redress increases across different areas of society dependent on the use of digital technologies, exposing a digital justice gap.[1] From extensive surveillance project to algorithmic discrimination, one of the primary questions of the algorithmic society focuses on effective remedies.[2] Where interactions are increasingly taking place in the digital realm, ensuring that individuals and communities have the means to seek justice and redress for a wide range of digital grievances is of paramount importance.

In the European constitutional framework, access to remedies, and their effectiveness, are guaranteed as a fundamental right. Since the entry into force of the Treaty of Lisbon, Article 47 of the Charter of Fundamental Rights (CFR) enshrining the right to an effective remedy became applicable alongside the general principle of EU law, and then shaped by the CJEU from notions of effectiveness and obligations of sincere cooperation of the Member States under Article 19(1) TEU.[3] In the European Union's emerging algorithmic society, the established constitutional fabric of this right however stretches with novel constellations of remedial avenues for the enforcement of individual rights emerging from the EU's digital acquis.

Fragmentation in the emerging remedial design is particularly problematic when considering the intersection of rules under the various digital legislative frameworks. For instance, a violation of the upcoming Artificial Intelligence Act, designed to regulate artificial intelligence technologies, will also apply to aspects of content moderation and, by extension, come under the obligations of the Digital Services Act. Similarly, the right against automated decision-making enshrined in the General Data Protection Regulation can serve as a basis for lodging complaints against violations of the AI Act. This interplay of legal instruments underscores the intricate system of rights and remedies that all of the actors involved in the remedial constellation,

---

[1] Orna Rabinovich-Einy and Ethan Katsh, *Digital Justice Technology and the Internet of Disputes* (Oxford University Press 2017).

[2] See the authors' contributions on the topic in Simona Demková, Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice (Edward Elgar Publishing 2023) and Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society (Cambridge University Press 2022).

[3] Pekka Aalto and others, 'Article 47 – Right to an Effective Remedy and to a Fair Trial', *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014).

including the private persons, the companies and other controllers, as well as the supervisory authorities, including the courts, will need to navigate in the digital age. Against this background, this work assesses the European regulatory approach to remedies in the digital policy. Through a careful analysis of the emerging remedial constellations, it demonstrates how, despite new remedial systems, the regulatory approach furthers the already-existing fragmentation and uncertainty. As a result, the effectiveness of remedies in the European algorithmic society firmly depends on the extent to which legislators can instil clear and efficient institutional collaboration, supported by the capacity of private actors, administrative authorities and courts to cooperate in the enforcement of EU law, above all, in a way that strengthens the protection of fundamental rights.

The paths paved for remedies within the EU's digital policy in this light seem to hit the thin line between the rights that are effective in law *and* in practice.[4] Taking a closer look at the legislative constellations of remedial procedures through the constitutional lens of the right to an effective remedy, this works argues that, as one of the cornerstones of the EU's constitutional set-up, the right to an effective remedy must be not only formally recognised through new procedures but also substantively protected by providing coordinated remedial systems within the Union's emerging algorithmic society. Therefore, this work assesses to what extent the emerging legislation preserves the right's constitutional fabric in the algorithmic society.

To that end, the contribution first sketches the contours of the right to an effective remedy (section 2), before turning to the analysis of the fragmented landscape of remedies in EU digital policy (section 3). We assess the design, nature and limits of the remedies established under different instruments that can be classified as 'internal complaints', 'independent supervision' and 'judicial remedies'. In section 4, we highlight the key areas that require further clarification in order to ensure that the emerging digital *acquis* respect the constitutional right to an effective remedy.

[4] Following the requirement reaffirmed by the ECtHR, in *Kudla v Poland* [2000], Application No. 30210/96, 2000, para 157.

2. The Constitutional Fabric of the Right to an Effective Remedy

Since the entry into force of the Treaty of Lisbon, the right to an effective remedy became applicable alongside the general principle of EU law.[5] With 'codification' in Article 47 CFR, the right to an effective remedy has evolved as an independent 'right of EU rights',[6] demarcating the requirements for the protection of fundamental rights and freedoms under EU law.[7] Fleshing out the constitutional fabric of the right to an effective remedy is particularly challenging due to the its multifaceted nature. Its constitutional fabric stretches beyond the ambit of the Charter's application, towards the broader system of the judicial protection in the EU legal order by determining the EU and Member States' remedial regimes.[8]

The Court of Justice (CJEU) developed the right to an effective remedy from notions of effectiveness and obligations of sincere cooperation of the Member States under Article 19(1) TEU in conjunction with Article 4(3) TEU.[9] In this constellation, the Member States are obliged to ensure that the law is observed through effective legal protection in the fields covered by Union law, the latter requiring also structural guarantees of judicial independence and separation of powers within Member States. In latter respect, the late jurisprudence of the CJEU stresses that, as a general principle of EU law, effective judicial protection constitutes the 'essence' of the rule of law of the EU legal order.[10]

---

[5] Simona Demková and Herwig CH Hofmann, 'General Principles of Procedural Justice' in Katja Ziegler, Päivi Neuvonen and Violeta Moreno-Lax (eds), *Research Handbook on General Principles of EU Law: Constructing Legal Orders in Europe* (Edward Elgar Publishing 2022) 212.

[6] Matteo Bonelli, Mariolina Eliantonio and Giulia Gentile, 'Conclusions', *Article 47 of the EU Charter and Effective Judicial Protection: Volume 2: The National Courts' Perspectives:* (Hart Publishing 2023) 274.

[7] Herwig CH Hofmann and Bucura Catalina Mihaescu-Evans, 'The Relation between the Charter's Fundamental Rights and the Unwritten General Principles of EU Law: Good Administration as the Test Case' (2013) 9 European Constitutional Law Review 73.

[8] Kathleen Gutman, 'The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?' (2019) 20 German Law Journal 884.

[9] Article 4(3) TEU states: '[p]ursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure.'

[10] Case C-64/16 *Associação Sindical dos Juízes Portugueses* [2018] ECLI:EU:C:2018:117, para 36; Case C-216/18 PPU *Minister for Justice and Equality v LM* [2018] ECLI:EU:C:2018:586, para 51; Case C-72/15 *Rosneft* [2017] ECLI:EU:C:2017:236, para 73.

The latin maxim of *ubi ius, ibi remedium* demands that where there is a right under Union law, there is a remedy to ensure its enforcement.[11] Beyond the enforcement of individual rights, EU law guarantees to individuals 'the right to challenge before the courts the legality of any decision or other national measure relating to the application to them of an EU act'.[12] Thus, the guarantee of effective remedy entails both demands on effective access to the remedial avenues as well as the effectiveness of the remedy itself. In order words, EU legislators and Member States must design and facilitate individuals' access to remedial procedures for complaints concerning violations of EU law and ensure that the procedures are effective in law and in practice.

The national rules governing the right to complain are subject to the principle of national procedural autonomy.[13] Pursuant to the well-established *Rewe* line of case law,[14] however, the Court limits this procedural autonomy with the conditions of effectiveness and equivalence. The condition of effectiveness obliges Member States to establish the procedures in a way compatible with the Union law.[15] To that end, Member States must not 'render virtually impossible or excessively difficult the exercise of rights' conferred by EU law.[16] This entails both legal and practical possibilities for admissibility and the prospect of effectively hearing a claim and rendering a substantive remedy on the merits.[17]

[11] Demková and Hofmann (n 5) 212.

[12] Case C-64/16 *Associação Sindical dos Juízes Portugueses*, paras 35, with reference to Case C-583/11 *Inuit* [2013] ECLI:EU:C:2013:625, paras 91, 94.

[13] Anthony Arnull, 'Article 47 CFR and National Procedural Autonomy' (2020) 45 European Law Review 681.

[14] Case 33/76 *Rewe* [1976] ECLI:EU:C:1976:188, para 5; Case 45/76 Comet [1979] ECLI:EU:C:1976:191, para 12; Case 106/77 *Simmenthal* [1978] ECLI:EU:C:1978:49, paras 21–22; Case C-213/89 *Factortame* [1990] ECLI:EU:C:1990:257, para 19; Case C-312/93 *Peterbroeck* [1995] ECLI:EU:C:1995:437, para 12; and, more recently, 24 June 2019, Case C-619/18 *Commission v Poland (Independence of the Supreme Court)* [2019] ECLI:EU:C:2019:531, para 48 and Case C-64/16 *Associação Sindical dos Juízes Portugueses,* para 34.

[15] Treaty on the European Union (TEU), Art. 4(3).

[16] Case C-312/93 *Peterbroeck* [1995] ECLI:EU:C:1995:437, para 14 and Joined Cases C-430 and 431/93 *Van*
Schijndel [1995] ECLI:EU:C:1995:441, para 19.

[17] For a detailed commentary, see Herwig CH Hofmann, 'The Right to an Effective Remedy and to a Fair Trial - Article 47 of the Charter and the Member States' in Steve Peers, Tamara Harvey and Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart Bloomsberg 2019).

The requirement of ensuring effective access to remedies is not an 'unfettered prerogative'.[18] Indeed, the CJEU accepts as legitimate national rules that impose additional admissibility requirements, such as the requirement to first exhaust administrative complaint mechanisms.[19] In the case of *Puškár*, the CJEU approved the Slovak law requiring that breaches of the rights of data subjects must at first instance be brought before the data protection authority. According to the Court, the rationale of this limitation on the right to a judicial remedy is legitimate in view of reducing additional burden on the national courts, seeing it as ultimately contributing rather than undermining the efficiency of the judicial procedure.[20] In other words, EU law guarantees judicial remedy only as the final or ultimate remedy. Instead, to complement the inherent limits of court proceedings, the right to an effective remedy will be respected where the review by independent administrative bodies is effective in addressing potential violations of EU law.[21]

Lastly, the effectiveness of remedies overlaps with the guarantees stemming from the 'umbrella' right to good administration, enshrined in Article 41 CFR.[22] These guarantees of specific application to public administrations, include the duty of care, the right of access to one's files, the right to be heard or the right to a reasoned decision. The competent authority must exercise due care in decision-making, demonstrated through the statement of reasons for the adopted decision.[23] The statement of reasons for a specific decision enables the individual to understand the basis of that decision. Thus, as repeated by the CJEU, individuals may decide, 'with full knowledge of the relevant facts, whether there is any point in applying to the court with jurisdiction.'[24] At the same time, the statement of reasons puts the court 'in a position in which it may carry out the review of the lawfulness' of the decision in question.[25]

[18] Joined Cases C-317/08 to C-320/08 *Alassini* [2010] ECLI:EU:C:2010:146, para 63.
[19] Case C-73/16 *Puškár* [2017] ECLI:EU:C:2017:725.
[20] Hilde K Ellingsen, 'Effective Judicial Protection of Individual Data Protection Rights: Puškár' (2018) 55 Common market law review 1879.
[21] Simona Demková, Automated Decision-Making and Effective Remedies (n 2) 58–59.
[22] Demková and Hofmann (n 5).
[23] Joana Mendes, 'The Foundations of the Duty to Give Reasons and a Normative Reconstruction' in Elizabeth Fisher, Jeff King and Alison Young (eds), *The Foundations and Future of Public Law: Essays in Honor of Paul Craig* (Oxford University Press 2020).
[24] Joined Cases C-225/19 and C-226/19 *R.N.N.S., K.A. v Minister van Buitenlandse Zaken* [2020] ECLI:EU:C:2020:951, para 43.
[25] Ibid.

The simultaneous application of the above remedial rules as general principles of EU law means that they bind the authorities even where not explicitly required by the legislation in question.[26] Cumulatively, the guarantees of good administration in conjunction with the requirements of Article 47(1) CFR warrant the quality and integrity of decision-making procedures, allow individuals to know the factual basis for decisions concerning them and decide about their chances of obtaining correction or compensation in cases of violation of their rights by seeking remedies. The logic of the prerequisite requirements of good administration to ensuring effective remedies is widely mirrored within the transparency and accountability safeguards enshrined in the Union's emerging digital *acquis*.[27]

The algorithmic age however demands a more refined remedial framework beyond judicial remedies. Indeed, the emerging EU digital *acquis* establish an extensive array of *ex ante* accountability mechanisms, including impact assessments, continuous reporting and informing duties, or horizontally applicable common technical standards. As argued elsewhere,[28] not all of these mechanisms constitute direct remedies. The latter can take different forms in the chain of remedial actions, culminating with the individual's right to a remedy before the court. Combinations of administrative and judicial review mechanisms are widely spread across EU policy areas. As the CJEU clarified in the case of *Puškár*,[29] rules prescribing an obligation to first exhaust administrative mechanisms before seeking a judicial review constitute legitimate limits on the right to an effective judicial protection. These rules reduce the burden already placed on the courts, thus ultimately reinforce the efficiency rather than weaken the remedies.

However, independent administrative supervision is also limited in the digital age due to the power increasingly exercised by private actors, such as online platforms. As a result, additional remedial constellations have become necessary in the algorithmic society, including 'private' internal complaint mechanisms. Indeed the latter now constitute one of the first and most accessible avenues for the enforcement of individual rights in the algorithmic society. Accordingly, the set up and functioning

[26] Case C-166/13 *Mukarubega v Seine-Saint-Denis* [2014] ECLI:EU:C:2014:2336, paras 43–9; Case C-521/15 *Spain v Council* [2017] ECLI:EU:C:2017:982, para. 89; C-604/12 *N* [2014] ECLI:EU:C:2014:302, para 49.

[27] Simona Demková, Melanie Fink and Giulia Gentile, 'Symposium on Safeguarding the Right to Good Administration in the Age of AI' (*The Digital Constitutionalist*, 3 October 2023) <https://digi-con.org/symposium-on-safeguarding-the-right-to-good-administration-in-the-age-of-ai/>.

[28] Demková, Automated Decision-Making and Effective Remedies (n 2) 55.

[29] Case C-73/16 *Puškár* [2017].

of such internal complaint mechanisms should be subject to a close scrutiny under the constitutional lens of the right to an effective remedy as well. The question then arises whether and to what extent the emerging complexity in the remedial procedures meets the requirements of the constitutional right to an effective remedy.

3. Remedial Constellations for the Digital Age

The Union has expanded its regulatory intervention in the digital age. At least, three landmark legislative frameworks, set up under the EU General Data Protection Regulation,[30] the Digital Services Act (DSA)[31] and the upcoming Artificial Intelligence Act,[32] constitute a milestone in the European approach to governing the digital age. These legislative frameworks are part of the EU's broader strategy on the Digital Single Market,[33] including many additional instruments, such as the Copyright Directive,[34] the amendments to the Audiovisual Media Services Directive,[35] the

[30] 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 [2016] OJ L (hereafter, the 'GDPR').

[31] 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 [2022] OJ L 277, (hereafter the 'DSA').

[32] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final, (AI Act Proposal). This chapter was finalised in January 2024 and is based on the latest consolidated draft of the AI Act, updated according to the provisional political agreement reached at the fifth trilogue between 6 and 8 December 2023, which was published by the Belgian Council presidency on 26 January 2024, available at: <https://media.licdn.com/dms/document/media/D4E1FAQEkEmsiFsvblw/feedshare-document-pdf-analyzed/0/1706538693071?e=1707350400&v=beta&t=vNT5eRsudctThJk3RT1m2MOMOyJlAnEQ56dyqm6DS7o>, hereafter referred to as 'AI Act'.

[33] European Commission, Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' (COM/2015/0192 final).

[34] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, [2019] OJ L 130.

[35] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJ L 95.

regulation to address online terrorist content.[36] These are only some of the examples of legal instruments adopted in recent years, which cumulatively bring about a change of paradigm aimed to provide new rules and safeguards to address the challenges raised by the algorithmic society.[37]

Nonetheless, this critical step in the European digital policy has not only led to the expansion of safeguards and remedies but also to their fragmentation and overlap. Taking a closer look into the remedial constellations under the GDPR, the DSA and the AI Act, it is possible to observe a horizontal trend in remedial fragmentation that is doomed to undermine the respect for the constitutional right to an effective remedy. Although all three legal frameworks aim to protect European values, including fundamental rights, their underlying remedial designs differ from each other, raising questions about the effectiveness of the remedies, and, more broadly, access to justice in the digital age. Their comparative assessment demonstrates procedural fragmentation across all three legal frameworks, which ultimately could frustrate the right of access to remedies, including judicial review. To illustrate the common pitfalls in these remedial constellations, the following discussion focuses on three types of remedies that exist under the EU digital *acquis*: the 'internal complaints', 'independent supervision', and 'judicial remedies'.

3.1. Internal Complaints

The provision of internal complaint-handling systems is a critical dimension of remedies, and, more in general, private ordering.[38] Not a novelty of the digital age, even if amplified in the latter context,[39] the expansion of private ordering has raised opportunities and challenges to regulate access to remedies, usually by terms of services.[40] Internal complaint-handling systems empower individuals and entities with alternative channels to address violations of their rights without relying on traditional system of administrative and judicial review. Particularly, internal

[36] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172.
[37] Hans-W. Micklitz and others (eds), Constitutional Challenges in the Algorithmic Society (Cambridge University Press 2020).
[38] Tehila Sagy, 'What's So Private about Private Ordering?' (2011) 45(4) Law & Society Review 923.
[39] Margaret J. Radin and R. Polk Wagner, 'The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace' (1999) 73 Chicago-Kent Law Review 1295.
[40] João Pedro Quintais, Giovanni De Gregorio, João C. Magalhães, 'How Platforms Govern Users' Copyright-Protected Content: Exploring the Power of Private Ordering and its Implications' (2023) 48 Computer Law & Security Review 105792.

complaint-handling systems provide more efficient access to remedies and an avenue to voice concerns and seek resolutions without immediately resorting to external legal action. They are designed to empower individuals to take control of the resolution process within an organisation, allowing users to make decisions about how their concerns should be addressed.

Nonetheless, internal systems can also be the source of serious challenges for individuals. First, transparency and accountability in the resolution of disputes lies in the hands of the private actors who are the governors of a given system. Internal handling systems could lead to quicker and accessible remedies but *de facto* opaque and unaccountable in their output. Second, these systems could be less open than judicial and administrative remedies, thus leading to increased discrimination among users while also diluting the efforts of public actors to provide effective remedies. This challenge is also connected with the questions around expertise in adjudication. Administrative and judicial authorities are usually better equipped to handle complaints and violation of rights. Although, considering the scale of possible complaints, the latter may lack the necessary technical capacity and expertise to do so effectively.

In the field of data, the GDPR has been welcomed as a tool that reinforces data subject's rights and the possibility to rely on more protection of personal data. While the GDPR does not provide for internal complaint mechanisms as a form of direct remedy akin to the type launched under the DSA, it does establish obligations on the data controllers, which enable individuals' access to remedies. Notably, key enablers of remedies under the GDPR are data subject's rights, particularly the right to access and the right of erasure.[41] According to the GDPR,[42] the data controller must provide the data subject with information, including, about their right to request from the controller rectification, erasure or restriction on the processing of their personal data. Similarly, the controller must inform the data subjects of their right to object to such processing and the right to lodge a complaint with a supervisory authority. As affirmed by the CJEU, this right of access is an essential enabler for the exercise of data subjects' rights in the digital age.[43] And the centrality of data subjects' rights is also underlined by the expansion of the intermediation to access remedies.[44] Indeed,

[41] Helena U. Vrabec, *Data Subject Rights under the GDPR* (Oxford University Press 2021).

[42] GDPR, Arts 15-22.

[43] Case C-553/07 *Rijkeboer* [2009] ECLI:EU:C:2009:293, paras 51-52.

[44] Alexandra Giannopoulou, Jef Ausloos, Sylvie Delacroix, Heleen Janssen, 'Intermediating data rights exercises: the role of legal mandates' (2022) 12(4) *International Data Privacy Law* 316.

closely related is the debate about the existence, or not of a so-called right to explanation under the GDPR's access to information rights.[45] As discussed below, the AI Act would put a full stop to that question by explicitly enshrining the right to explanation under Article 68(c).

More explicitly, however, the GDPR provides a mechanism for internal complaints with the role of a data protection officer,[46] who will be responsible for internal oversight of compliance with the data protection rules. The DPO can thus act as a recipient of internal complaints regarding the company's data processing activities.[47] Indeed, the CJEU considers the role of the DPO as essential to an effective remedy under Article 47 CFR. Notably, as affirmed in the landmark ruling in *Ligue des Droits Humains*,[48] 'the lawfulness of all automated processing must be open to review by the data protection officer and the national supervisory authority, […] as well as by the national courts in the context of the judicial redress'. To that end, the CJEU extends the requirement of providing the national supervisory authorities with sufficient material and human resources necessary to carry out their review also with respect to data protection officers.[49] Similarly, according to the Court, the DPO should be able to exercise its tasks with sufficient functional independence, including protection from unjustified termination of DPO's appointment by the employer.[50]

In the field of content moderation, the DSA has brought about a significant expansion of the remedies available to users and other recipients who wish to lodge complaints against violations of their rights by and on online platforms. Compared to its predecessor – the e-Commerce Directive, which primarily focused on exempting online intermediaries from liability but did not provide substantial remedies against discretionary content moderation decisions, the DSA introduces a more comprehensive approach. The DSA emphasises not only the need for timely and diligent content moderation but also the necessity for robust safeguards to protect the

[45] See notably, Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18; Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143.

[46] Article 37 GDPR.

[47] GDPR, Article 38(4), '[d]ata subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation'.

[48] Case C-817/19 *Ligue des droits humains v Conseil des ministres* [2022] ECLI:EU:C:2022:491, para 179.

[49] Ibid, para 180.

[50] GDPR, Art. 38(3), see Case C-534/20 *Leistritz AG v LH* [2022] ECLI:EU:C:2022:495, paras 27-28.

rights and legitimate interests of all parties, particularly their fundamental rights, including the right to an effective remedy.[51]

The DSA introduces a multi-layered system of remedies with two main options: internal complaint-handling systems and out-of-court dispute settlement. Importantly, these remedies do not exclude the possibility of resorting to courts and administrative remedies. Under the DSA,[52] contesting decisions of providers of online platforms through internal mechanisms should not prevent the individuals' possibility to seek judicial redress, thus ensuring the right to an effective judicial remedy under Article 47 CFR.

The DSA extends access to remedies not only to users but also to a broader category of 'recipients', which includes 'any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible'.[53] This approach expanded personal scope encompasses not only users affected by content moderation decisions but also third parties who may want to report content issues. This applies to decisions that uphold or dismiss such reports, ensuring that both users and third parties have access to remedies against content moderation decisions.

Online platforms are required to introduce internal complaint-handling systems for claims against the publication of illegal content, or at least content incompatible with its terms and conditions. For a period of at least six months following specific content moderation decision, particularly on whether to remove or disable access to or restrict visibility of the information; to suspend or terminate the provision of the service, in whole or in part, to the recipients; to suspend or terminate the recipients' account; suspend, terminate or otherwise restrict the ability to monetise information provided by the recipients.[54]

The DSA demands that online platforms treat complaints in a timely, non-discriminatory, diligent, and non-arbitrary manner, although it does not provide specific guidance on these requirements. Instead, the DSA leaves the discretion to platforms to define their own standards, which can be a point of contention, especially

[51] Aleksandra Kuczerawy, *Remedying Overremoval: The Three-Tiered Approach of the DSA, VerfBlog*, 3 November 2022, available at: https://verfassungsblog.de/remedying-overremoval/.
[52] DSA, Recital (59).
[53] Ibid, Art. 3(b)
[54] Ibid, Art. 40.

in cases involving political speech. This rule leaves space to online platforms to achieve a decision that defines a fair outcome.[55] Online platforms are also under pressure to reverse decisions when a notice is deemed unfounded, or the content is not illegal, incompatible with their terms and conditions or contains information indicating that the complainant's conduct does not warrant the measure taken. Even when a complaint is not upheld, online platforms must provide a reasoned decision and inform users about the availability of out-of-court dispute settlement systems and other forms of redress, including judicial remedies.

The DSA also introduces a critical safeguard in this process by requiring online platforms not to make decisions on complaints solely based on automated means. Online platforms have to rely on the supervision of qualified staff who will be responsible for the mechanism of internal complaints. As a result, artificial intelligence technologies cannot exclusively drive this redress mechanism. This safeguard is critical to ensure that those recipients which have already been subject to an automated decision about the removal of their content are not again judged by another automated system. The limit on automation in the review of these decisions is a challenge for online platforms considering the potential number of requests but it is also critical to ensure that this procedural safeguard is not diluted by another automated assessment.

In contrast, individual remedies were not envisioned in the original proposal for the Artificial Intelligence Act advanced by the European Commission in 2021. Instead, as stated in the Preamble, the rules of the AI Act 'should apply without prejudice to existing Union law.'[56] Accordingly, as Union and national law 'already provides effective remedies to natural and legal persons,' individuals should avail themselves of the existing remedies also where their 'rights and freedoms are adversely affected by the use of AI systems'.[57] This is because, since its inception, the AI Act was drafted as a product-safety regulation, which builds on demands for developing internal accountability culture by the AI providers and deployers as the means to compliance with the Act's requirements. The resulting consolidated text of the AI Act therefore seems to assume a complementary role in addition to the existing Union laws, especially fundamental rights protection.

[55] Ibid, Recital (58).

[56] AI Act, Preamble (5a).

[57] AI Act, Preamble (84aa).

Internal accountability requirements that arise from the AI Act thus differ substantially from the direct complaint-handling mechanisms introduced by the DSA and even from the indirect remedial role played by the figure of Data Protection Officer under the GDPR. Indeed, the AI Act does not envision a similar figure of an AI Officer to be responsible for the company's compliance with the new rules. Instead, the Act aims at creating a horizontal compliance culture across the companies' chain of responsibilities enforced through the market certification procedures.

Nonetheless, the latest consolidated version of the agreement on the Act includes a rather limited right of AI subjects to complain against the AI systems' potential misuses.[58] On the one hand, affected individuals may bring complaints before the national market surveillance authority as a form of administrative remedy, as discussed in the next section. On the other hand, subjects of AI uses should also be able to have access to internal review through the newly introduced right to explanation. Particularly, anyone affected by a decision made by the deployer based on the output from a high-risk AI system that significantly impacts their health, safety, and fundamental rights has the right to request a clear and meaningful explanation from the deployer on the role of the AI system in the decision-making process and the main elements of the decision.[59]

In addition, pursuant to the general obligations under the AI Act falling on the deployers and the providers and users of the high-risk AI systems in individual decision-making,[60] the affected person must be informed that they are subject to the use of such a system. Although with the usual exception for the context of law enforcement context, the providers and users of such systems must inform the concerned natural persons in a clear and distinguishable manner at the latest at the time of the first interaction or exposure to the system.[61]

As already hinted-at above, this provision might give a full stop to an academic debate about the existence or non-existence of the right to explanation under the parallel information rights of the GDPR,[62] and the underlying requirements of disclosure of

[58] AI Act, Chapter 3b Remedies. See the discussion in section 3.2 below.
[59] AI Act, Chapter 3b Remedies, Art. 68(c).
[60] AI Act, Article 29(6b) 52(1).
[61] AI Act, Article 52(3a).
[62] GDPR, Articles 13(2)(f) and 14(2)(g) and 15(1)(h). For different views on the topic, see Edwards and Veale (n 45); Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243; Paul De Hert and Guillermo Lazcoz, 'Radical Rewriting of Article 22 GDPR on Machine

the algorithmic logic as well as the significance and the envisaged consequences of automated processing for the data subject. The AI Act's right to explanation however seems to be formulated in a similarly ambiguous fashion to the information rights under the GDPR with respect to the key question mark about the impact of the use of an AI system on the decision-making process.

Recently, this aspect was also addressed for the first time by the CJEU. Notably, in the case of Schufa Holding,[63] the Court established that the automated calculation of a probability rate based on personal data constitutes an automated decision-making process in the sense of Article 22(1) of the GDPR when a third party heavily relies on such probability value to establish, implement, or terminate a contractual relationship with an individual. However, here, the Court's interpretation aligns with the object of the GDPR's provision,[64] which explicitly mentions the automatic refusal of an automated credit refusal. This evaluation is considered a form of "profiling" aimed at assessing personal aspects related to a natural person. As such, this ruling does not seem to provide the necessary guidance for assessing the effects of AI-driven automation on decision-making processes in other contexts.[65]

The question how to operationalise the right to a meaningful explanation as a form of internal remedy therefore remains open, especially as regards the application of the new right under the AI Act vis-à-vis its equivalents in the GDPR.[66]

Decisions in the AI Era' (*European Law Blog*, 13 October 2021) <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/>.

[63] Case C-634/21 *Schufa Holding AG* [2023] ECLI:EU:C:2023:957. See also the analysis of the decision by Francesca Palmiotto, 'Op-Ed: " 'Scoring' for Data Protection Rights: The Court of Justice's First Judgment on Article 22 GDPR (Case C-634/21 and Joined Cases C-26/22 and C-64/22)"' (*EU Law Live*, 9 January 2024) <https://eulawlive.com/op-ed-scoring-for-data-protection-rights-the-court-of-justices-first-judgment-on-article-22-gdpr-case-c-634-21-and-joined-cases-c-26-22-and-c-64-22-by/>.

[64] GDPR, Preamble (71) specifies that a 'data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, *such as automatic refusal of an online credit application* or e-recruiting practices without any human intervention.' (Emphasis added).

[65] Such as in the law enforcement context. Contrast with the already mentioned ruling in *Ligue des droits humains* [2022], para 194, where the Court expressed reservation towards the use of a specific type of AI systems, namely self-learning or machine learning systems in advanced assessment of the risk of air passengers under the PNR Directive (EU) 2016/681.

[66] See section 4.1 below.

3.2. Independent Supervision

Independent supervision lies at the core of the Union's multilevel accountability system across different policy areas. The vast magnitude and diversity of potential harmful activities in algorithmic society would affect individual rights and interests, renders judicial review not a viable option.[67] Given the demands of the algorithmic age, it is presumed that independent supervision constitutes the cornerstone in the system of remedies.

As recalled above, the CJEU also clarifies that rules prescribing an obligation to first exhaust the administrative complaint mechanisms before seeking a judicial remedy constitute legitimate limits on the right guaranteed in Article 47 CFR.[68] On the contrary, the Court understands administrative review mechanisms to enhance the efficiency of the court proceedings by reducing the burden where claims can be sufficiently handled on substance by administrative bodies, provided that these does not cause disproportionate burden, such as costs and time, on the parties.[69]

Two key aspects determine the compatibility of administrative review mechanisms with the essence of the constitutional right to an effective remedy: its complete independence; and the practical arrangements for the exercise of such remedies so as not to disproportionately affect the right to an effective remedy before a court. Both aspects have been extensively deliberated by the Court in its jurisprudence.

Regarding the requirement of independence, the CJEU echoes the understanding of the word as one referring to 'complete independence',[70] in the form of both formal detachment from other branches of the government so as to prevent both direct and indirect influence, as well as practical, often discussed as 'functional',[71] or 'operational',[72] independence, evidenced by the supervisory authorities' legal powers

[67] Jennifer Cobbe, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making' (2019) 39 Legal Studies 636.

[68] Case C-73/16 *Puškár* (n 19) para 67.

[69] Ibid, para 70 with references to previous case-law Joined Cases C-317/08 to C-320/08 *Alassini and Others* [2010] ECLI:EU:C:2010:146, para 67, and of 14 June 2017, Case C-75/16 *Menini and Rampanelli* [2017] ECLI:EU:C:2017:457, para 61.

[70] See the relevant case-law: namely, Case C-518/07 *European Commission v Germany* [2010] ECLI:EU:C:2010:125, paras 23–25; Case C-362/14, *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 57.

[71] Case C 614/10 *European Commission v Austria* [2012] ECLI:EU:C:2012:631, para 41.

[72] Case C 288/12 *European Commission v Hungary* [2014] ECLI:EU:C:2014:237, para 52.

and sufficient resources to exercise effective oversight. Regarding the practical arrangements, the obligation to exhaust additional administrative remedies constitutes a legitimate precondition for bringing a legal action, as long as it meets the test in Article 52(1) CFR. Namely, such precondition must be provided for by law, respect the essence of the right to an effective remedy and, be proportionate to the objectives of EU's general interest or the need to protect the rights and freedoms of others.[73]

The GDPR provides a general right to lodge a complaint with a supervisory authority.[74] Accordingly, the data subjects can access a direct remedy against violation of their rights that is normally free of charge. Although this remedy could not lead to the same effects as judicial remedies in terms of ordering a compensation of damages,[75] administrative review plays a critical deterrent for data controllers by the DPAs' power to impose substantial administrative fines for non-compliance with the GDPR.[76] Indeed, administrative remedies allow data subjects to make their voices be heard and thus exercise the autonomy over their data and privacy.

The primary limit of administrative supervision lies in the different capacities of data protection authorities across Member States.[77] As in other fields such as consumer law, fragmentation of enforcement authorities in the field of data protection could impact how data subjects access remedies across the Member States, considering the different institutional setting and resources of administrative authorities. This situation might lead to different levels of protection of personal data across the EU.

Under the DSA, users, also represented by any body, organisation or association on their behalf akin to the GDPR practice,[78] have the right to lodge a complaint with the Digital Services Coordinator against providers of intermediary services alleging an infringement of the DSA. The competent digital services coordinator of the Member State where the recipient of the service is located or established will have to address the raised grievance and inform the other coordinators as well as the Commission on

[73] Joined Cases C-439/14 and C-488/14 *Star Storage and Others* [2016] ECLI:EU:C:2016:688, para 49.
[74] GDPR, Art. 77.
[75] GDPR, Art. 82(6).
[76] But see Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' (2022) 12 International Data Privacy Law 1.
[77] Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 International and Comparative Law Quarterly 799.
[78] GDPR, Art. 80.

the resolutions adopted.[79] This right gives the possibility to users to notify the supervision authority about a violation of the DSA, also extending the role of collective remedies.

Besides the complaints to the Digital Service Coordinators, the DSA grants the users the possibility to access an out-of-court dispute resolution mechanism.[80] By relying on an entity certified to address disputes as defined by Digital Service Coordinators, access to remedies is still possible for complaints that have not been resolved through the internal complaint-handling system. In any case, accessing out-of-court dispute mechanisms does not affect the recipient's right to initiate legal proceedings against online platform providers at any point. In this case, the out-of-court dispute bodies are required to make their decisions available to the involved parties within a reasonable period of time and no later than ninety calendar days after the receipt of the complaint. In the case of highly complex disputes, the certified out-of-court dispute settlement body may, at its own discretion, extend the period for a maximum total duration of 180 days.

The primary challenge of this system comes from the freedom of online platform providers to refuse to engage with certified bodies if a dispute regarding the same information and grounds of alleged illegality or content incompatibility has already been resolved. This issue could not only lead to a fragmentation of approaches,[81] but also dilute the effectiveness of this remedy. While recipients can still access a judicial remedy, this system still leaves platforms free to argue that a certain content moderation decision has already been solved or dealt with other instruments. This leeway tends to increase conflicts, thus potentially limiting the effectiveness of this remedy.

Additionally, decisions made by certified dispute resolution bodies are not binding for the parties involved. This non-binding nature raises the question of whether online platforms will heed these decisions or opt to ignore them, potentially pushing recipients to seek judicial remedies for a binding review of content moderation decisions. This limitation inclines this remedy to be less effective and still leaves discretion for online platforms about not only formally granting access but substantially ensuring an effective remedy.

[79] DSA, Art. 53.

[80] DSA, Art. 21.

[81] Jörg Wimmers, The Out-of-court dispute settlement mechanism in the Digital Services Act - A disservice to its own goals, 12 (2021) JIPITEC 421 para 1.

For the AI Act, as already explained above, the legislators compensate the lack of direct remedies within its text by reaffirming the availability of the existing administrative and judicial remedies under Union and national law also to situations where natural persons consider that their rights and freedoms are adversely affected by the use of AI systems. Yet, the AI Act enshrines an additional form of administrative complaint mechanism for natural persons by granting the right to lodge a complaint to a national market surveillance authority where they consider that there has been a breach of the rules of the AI Act.[82] In such cases, the relevant market surveillance authority must follow the established procedures under the EU Market Surveillance Regulation.[83]

What appears the most problematic in the Act's remedial design is the resulting confusion in the administration of its independent supervision, especially where AI systems are used in individual decision-making that also relies on processing of personal data. By the *lex specialis* nature of the European data protection rules,[84] such competence should understandably lie with the national data protection authorities. Yet, in principle, it will be the market surveillance authorities that will be entrusted with the oversight of compliance with the AI Act before and after placing the products on the market.[85] This potentially entrusts market authorities with the power of hearing complaints from consumers and other private parties, by performing the 'appropriate checks'.[86] There is a lack of understanding about the extent to which these 'appropriate

[82] AI Act, Chapter 3b Remedies, Art. 68(a).

[83] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, [2019] OJ L 169.

[84] AI Act, Recital (5aa) states: 'This Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. […] It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling.'

[85] pursuant to the market surveillance powers granted under the general Market Surveillance Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, [2019] OJ L 169.

[86] Article 11 (3)(e) of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, [2019] OJ L 169.

checks' performed with respect to high-risk artificial intelligence products will be able to effectively address potential fundamental rights complaints.[87]

As a result of this multifaceted design, substantial fragmentation is likely to grow for the specific tasks and responsibilities in the *ex-post* enforcement of the AI Act. Depending on the context of the use of a specific artificial intelligence system, the competent supervisory authority in the Member State may vary.[88] Exceptions are further acknowledged wherever this is in the interests of cooperation. Similarly, for the AI systems used in the context of law enforcement, the supervisory powers should rest with the authority supervising the law enforcement activities.[89]

3.3. Judicial Remedies

Judicial remedies represent the ultimate form of remedy in constitutional democracies, including in the Union legal order, as guaranteed under Article 47 CFR. Access to a court inheres in the rule of law as an essential component of any democratic system.[90] It gives individuals and organisations the possibility to ask respect of the law, and, particularly, challenge the exercise of public or private powers. Within EU law, the critical importance of judicial (and administrative) remedies has been already underlined by the increasing trend of private enforcement in different areas from competition to consumer law.[91] This trend has also been characterising the expansion of regulatory approaches to private enforcement.[92]

The GDPR gives data subjects a two-fold possibility to seek judicial redress. On the one hand, data subjects can bring a complaint before a court concerning an alleged violation of the GDPR rules or their rights as data subjects by the data controller.[93] On the other hand, the GDPR further guarantees data subjects the right to seek a judicial

[87] See section 4.3 below.

[88] AI Act, Art. 63(4).

[89] AI Act, Art. 63(5).

[90] See ECtHR, *Golder v United Kingdom* [1975], Application no. 4451/70, para 34; more recently the CJEU's Cases C-72/15 *Rosneft* [2017] ECLI:EU:C:2017:236, para 73 and C-216/18 PPU *Minister for Justice and Equality v LM* [2018] ECLI:EU:C:2018:586, para 51.

[91] Miguel Sousa Ferro, 'Consumer Antitrust Private Enforcement in Europe' (2022) 13(8) *Journal of European Competition Law & Practice* 578; Rupprecht Podszun, 'Private Enforcement and Gatekeeper Regulation: Strengthening the Rights of Private Parties in the Digital Markets Act' (2022) 13(4) *Journal of European Competition Law & Practice* 254.

[92] Matthew Stephenson, 'Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies' (2005) 91(1) Virginia Law Review 93.

[93] GDPR, Art. 78.

remedy against the legally binding decision concerning them issued by the independent supervisory authority.[94] The latter scenario emerges where a supervisory authority fails to handle a complaint or does not inform the data subject within the prescribed time limit of three months regarding the progress or outcome of their complaint. This two-fold system of access to judicial remedies underscores the rights-based approach of the GDPR with the objective of ensuring a high level protection of the fundamental rights to private life and personal data protection under Article 7 and 8 CFR.[95] Recently,[96] the CJEU held that even where the supervisory authority provides only the minimum information on the outcome of a given investigation for the purposes of preserving the public interest of state security, the court must be able to examine the grounds and the evidence behind the supervisory authority's decision as a legally binding act. More recently, the CJEU also reaffirmed that data protection authorities' decisions on complaints from data subjects are subject a full judicial review, 'which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them'.[97] Essentially, this dual recourse to courts safeguards the right to an effective remedy as essentially an individual fundamental right.

The GDPR also grants a collective right of access to a court by allowing the data subject to mandate a not-for-profit body, organisation, or association properly constituted in accordance with the law of a Member State, to bring the complaint on their behalf.[98] Member States can furthermore grant designated bodies, organisations, or associations the right to independently lodge a complaint with the supervisory authority when they believe that a data subject's rights under GDPR have been violated due to processing. An important addition to the remedial architecture, especially considering the information and power asymmetry between the data subjects and data controllers in the digital age. Indeed, research shows that

[94] GDPR, Art. 79.

[95] Raphaël Gellert, 'Introduction: The Risk-Based Approach as the Opposite of the Rights-Based Approach, or as an Opportunity to Analyse the Links between Law, Regulation, and Risk?' in Raphaël Gellert (ed), *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

[96] Case C-333/22 *Ligue des droits humains* (Verification by the supervisory authority of data processing) [2023] ECLI:EU:C:2023:874.

[97] Joined Cases C-26/22 and C-64/22 *UF and AB v Land Hessen* [2023] ECLI:EU:C:2023:958, para 52, reinstating the role of due diligence in the review by the DPA addressed in Case C-311/18 *Facebook Ireland and Schrems* [2020] ECLI:EU:C:2020:559. See also the analysis of the judgment by Maria Magierska, 'No, the Data Protection Complaint Is Not a Petition' (*European Law Blog*, 25 January 2024) <https://europeanlawblog.eu/2024/01/25/no-the-data-protection-complaint-is-not-a-petition/>.

[98] GDPR, Art. 80.

individuals rarely exercise their GDPR rights, not to say seek judicial redress for any potential violations, which often incurs high costs.[99] It is therefore unsurprising that most high-level cases concerning the violations of the GDPR originate in complaints brought by the civil society organisations.[100] It is also a further reason why internal mechanisms may become the dominant avenue for remedies in the long run.

Similarly, the DSA introduces the right for users to access judicial remedies. Users have the right to seek compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations.[101] In guarantee of the right to an effective judicial remedy under Article 47 CFR, the DSA encourages, rather than itself affords, an explicit avenue for accessing courts.

The DSA leaves the possibility to national judicial and administrative authorities to order providers of intermediary services to remove specific illegal content or to provide certain specific information.[102] The latter form of judicial remedy in the online environment raises its own challenge due to the limited harmonisation in the national legal orders and the territorial limits of the national legal decisions concerning the online content.[103] The DSA is thus destined to face a similar enforcement challenge as the GDPR in cross-border cases, an area that triggered efforts for critical reform.[104]

---

[99] Gloria González Fuster and others, 'The Right to Lodge a Data Protection Complaint: OK, but Then What? An Empirical Study of Current Practices under the GDPR' (Data Protection Law Scholars Network and Access Now 2022) <https://www.accessnow.org/cms/assets/uploads/2022/06/Complaint-study-Final-version-before-design-June-15.pdf>.

[100] Including those resulting in landmark CJEU rulings, including the already-mentioned Case C-817/19 *Ligue des droits humains* [2022], with the exception of the 'individual' cases brought by Max Schrems in Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, which of course subsequently led to him to found one of the most active data protection NGOs in Europe – the 'noyb'. For an overview of the litigation raised by the latter, see noyb, [2023], Overview of noybs's GDPR Complaints, available at: <https://noyb.eu/en/project/cases>.

[101] DSA, Art. 54.

[102] DSA, Art. 10 and Recital (31).

[103] Dan Jerker B Svantesson, 'The Tyranny of Territoriality', *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017).

[104] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, [2023] COM/2023/348 final. See the discussion in section 4.3 below.

At the very least, the DSA encourages the provision of information on redress mechanisms available to both the provider of the intermediary services as well as to the uses of the services, including about both administrative complaint-handling mechanisms as well as judicial redress. Moreover, the DSA empowers the Digital Services Coordinators to develop national tools and guidance regarding the national complaint and redress mechanisms to facilitate users' access to such mechanisms.[105] Given that the right to an effective judicial remedy applies also as a general principle of EU law, such an omission in the remedial design is not in itself inconsistent with the requirements of the right in Article 47 CFR.

In contrast, the final agreement on AI Act does not enshrine an explicit right to seek judicial remedies against the uses of AI systems. Although the amendments advanced by the European Parliament included such a right, the trilogue seemed to conclude that acknowledging the judicial remedies already existing under Union law is sufficient.[106] Indeed, given the constitutional character of the CFR, the persons affected by the use of high-risk AI systems should in principle be able to seek judicial remedies where they consider their rights and freedoms protected under EU law are affected.

The same however would not hold true for the broader effects that the use of such systems might produce for instance on their health or safety, or other interests where the AI systems are put into use by private actors. In this respect, the only available mechanism to seek redress will likely entail the possibility to seek damages under the new Product Liability Directive,[107] in conjunction with the requirements under the new AI Liability Directive.[108] Ultimately, the access to judicial remedies is likely to be conditioned by the allocation of supervisory competences over AI uses that negatively affect individuals.

[105] DSA, Recital (39).

[106] AI Act, Chapter 3b Remedies.

[107] European Commission, (2022), Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final, see the latest developments summarised by Luca Bertuzzi, 'EU Updates Product Liability Regime to Include Software, Artificial Intelligence' (*www.euractiv.com*, 14 December 2023) <https://www.euractiv.com/section/digital/news/eu-updates-product-liability-regime-to-include-software-artificial-intelligence/>.

[108] European Commission, (2022), Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM/2022/496 final.

4. Fostering the Right to an Effective Remedy in the Digital Age

Ensuring respect for the right to an effective remedy in the digital age is a challenge of a particularly multi-faceted nature. Any discussion regarding efforts for improving the remedial designs needs to keep in mind the inherent limits of the right to an effective remedy in the digital age. Despite these inherent limits to ex-post remedies, the constitutional nature of the right to an effective remedy demands to strive at improving the available mechanisms. This implies both, fostering the conceptual clarity on the rules that pre-determine effective oversight, as well as fostering the institutional collaboration necessary under a fragmented legislative design.

4.1 Inherent Limits of Ex-post Remedies

In its case-law in the security context, the CJEU put forward first insights regarding the role and exercise of remedies in the algorithmic society.[109] Notably, the Court stressed the incompatibility of self-learning systems of artificial intelligence based on machine-learning technology with the requirements of the right to an effective remedy.[110] Thus, the Court underlined the importance of disclosure of sufficient information regarding the criteria used in automated assessments of individuals as well as about the programs applying those criteria in order to enable the individual 'to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress'.[111] These insights reaffirm the pre-condition of sufficient transparency, including through the statement of reasons, for the effectiveness of ex-post remedies.

[109] Joined Cases C-511/18, C-12/18 and C-520/18 *La Quadrature du Net* [2020] ECLI:EU:C:2020:791, para 182.
with reference to Opinion 1/15 (EU–Canada PNR Agreement) of 26 July 2017, ECLI:EU:C:2017:592, paras 173, 174, and most recently in the already-mentioned *Ligue des Droits Humains* [2022].

[110] *Ligue des Droits Humains*, para 194, the Court states that 'use of such technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive. […], given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter […].'

[111] Ibid, para 211.

However, these insights also reflect the limits of ex-post review of algorithmic conduct. In the given context, the CJEU insisted on the requirement of a prior review of the criteria for automated systems before they are put in place by a court or another independent supervisory authority. [112] While the latter may be too far-fetched a requirement for all types of algorithmic uses, transparency through ex-ante authorisation logic can be observed within the rules of the emerging digital *acquis*. For instance, the product-safety requirements of the AI Act oblige a prior authorisation through a conformity assessment and subsequent certification for any high risk artificial intelligence systems before they are placed on the EU's market. Moreover, the AI Act stipulates obligations on the providers and deployers of artificial intelligence systems to undertake a continuous review and verification of the compliance with the AI Act requirements, including through a new conformity assessment in cases of substantial modifications made to the system.[113] Without claiming to do justice here to the nuances of this complex topic, at least, three limits of ex-post, and especially judicial, remedies must be highlighted.

First, courts' jurisdiction continues to be construed along the territorial limits.[114] This characteristic leads to greater deference and collaboration among the national judicial and other supervisory authorities when applying the rules of the new digital *acquis* within their territories. As recalled above, the DSA's possibility of national judicial and administrative authorities to issue orders of content removal to intermediary services will hold implications beyond the territory of that authority's territorial jurisdiction. Accordingly, the DSA only provides minimum conditions on the form and nature of these national orders, focused on the obligation to inform the relevant authorities about the effect given to those orders for their efficient cross-border application.

Second, the scope of judicial review of compliance with the new digital *acquis* is limited, especially where it includes review of technical standards.[115] Pursuant to the

[112] Ligue des Droits Humains, para 223.

[113] AI Act, Art. 43. See also recitals (54), (62), (66), save in some exceptional circumstances as elaborated in art. 47, where judicial authorisation may be required for placing a certain AI system on the market for the purposes of the protection of life and health of persons, environmental protection or the protection of crucial infrastructure.

[114] Dan Jerker B Svantesson, 'Scope of (Remedial) Jurisdiction', *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017).

[115] Carlo Tovo, 'Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law' (2018) 55 Common Market Law Review <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2018096

ruling of the CJEU in *James Elliott*,[116] technical standards trigger only a limited scope of judicial review.[117] In this case, the Court expanded its jurisdiction to review technical standards as acts of private actors, through a teleological interpretation of Article 267 TFEU. A lot remains however unclear regarding the review of such instruments, including with respect to the disputes over their copyright protection, resolution on which is currently pending before the Court.[118] The Advocate General Medina in the latter case,[119] reaffirms the words of Advocate General Campos Sánchez-Bordona in *James Elliott,* that harmonised technical standards should be considered as 'acts of the institutions, bodies, offices or agencies of the European Union.'[120] Although this proposition was not explicitly accepted by the Court, Medina argues that there are good reasons to explicitly reconsider the nature of technical standards in light of their 'marked strategic interest for the EU' by increasingly incorporating 'core EU democratic values and interests, as well as green and social principles.'[121] Indeed, this holds even more true with respect to the technical standards for the digital age.[122] While the EU digital *acquis* provide for a 'fallback' option through granting the Commission with the power to adopt technical or common specifications via implementing acts in specific cases to protect public interests,[123] the question of the role of standardisation in ensuring protection of the Union's common values, including protection of fundamental rights remains open and pressing.

.pdf>; Mariolina Eliantonio and Annalisa Volpato, 'The European System of Harmonised Standards. Legal Opinion for ECOS' (Social Science Research Network 2022) SSRN Scholarly Paper 4055292 <https://papers.ssrn.com/abstract=4055292>.

[116] Case C-613/14, James Elliott Construction Limited v Irish Asphalt Limited [2016], ECLI:EU:C:2016:821.

[117] AI Act, Art. 40.

[118] Appeal brought on 23 September 2021 by Public.Resource.Org, Inc., Right to Know CLG against the judgment of the General Court (Fifth Chamber, Extended Composition) [2021] in Case T-185/19, *Public.Resource.Org, Inc. and Right to Know CLG v European Commission.*

[119] See Opinion of Advocate General Medina in Case C-588/21 P *Public.Resource.Org, Inc., Right to Know CLG v European Commission* [2023], ECLI:EU:C:2023:509.

[120] Ibid, points 16–18 with reference to Opinion in *James Elliott Construction* (Case C-613/14, ECLI:EU:C:2016:63, point 40).

[121] Ibid, point 21.

[122] Communication from the Commission, [2022] 'An EU Strategy on Standardisation – Setting global standards
in support of a resilient, green and digital EU single market', COM/2022/31 final, 2 February 2022, p 4.

[123] Ibid, p 5, see also AI Act, Art. 41.

Lastly, administrative and judicial remedies face a range of not-insignificant practical limits, such as time and costs of proceedings, as well as the lack of technical expertise in light of the opacity and informational power asymmetry in the algorithmic conduct. Furthermore, as stressed above, decisions made by certified dispute resolution bodies under the DSA are not binding for the parties involved, which will also affect their effectiveness in practice. Similarly, the direct individual complaint mechanisms under the GDPR and the AI Act may be more timely and costly, hence less accessible for the users to actually rely on.

The effectiveness of the remedy in the digital age becomes somewhat diluted due to these inherent limits of *ex post* oversight of algorithmic conduct by independent authorities, including the courts. While it might seem intuitive that having more rights would lead to enhanced protection for individuals, the reality is more intricate. The proliferation of rights and remedies poses a challenge for all the actors involved in the digital accountability infrastructure, from the private persons as the users and subjects of digital realm, the companies as the controllers, to supervisory authorities and the courts as the account-givers. For the users and subjects, the fragmentation means limited clarity on which specific remedy they can access in the event of a violation of their rights and freedoms. For the controllers or providers this entails a difficulty in designing the technical and organisational structures for the simultaneous compliance with the requirements of numerous legal frameworks. Lastly, for the supervisory authorities, the fragmentation creates a difficulty in applying and reviewing the compliance in light of numerous and inter-related legal obligations, also in light of the supervisory authorities' jurisdictional and other practical limits discussed here.

As stressed throughout this work, the right to an effective remedy is not solely a matter of protection of substantive rights. It also hinges on the existence of clear and practical avenues and actual possibilities for the enforcement of substantive rights. In other words, the prospect of respect for the right to an effective remedy is closely tied to a challenge stemming from the proliferation of rules and actors, each with its distinct competencies and functions. This situation impacts all layers of this right. In light of this scenario, it is of paramount importance to emphasise the need for clarity in the interplay between the legal frameworks. This clarity is necessary with respect to both the intra- and inter-framework interplay between the explainability obligations in a given algorithmic conduct, as preconditions for effective oversight, as well as regarding the provisions on institutional collaboration necessary for the coordination among the various remedies.

4.2 Fostering Clarity in the Interplay of Transparency Requirements

Effective access to remedies strongly depends on the clarity in the interplay between the emerging digital *acquis*. Indeed, the DSA and the AI Act apply in conjunction and without prejudice to the EU's data protection rules, the latter having the character of *lex specialis*.[124] A good example illustrating their interplay is the case of biometric and other sensitive personal data used for targeted advertising purposes, an activity governed by all three legal frameworks simultaneously.[125] All three legal frameworks aim to prohibit, or at least, strictly limit the harmful manipulative practice of targeted advertising based on processing of special categories of personal data, such as gender, political views, or sexual orientation.[126] Research, however, shows an increasing relevance of the use of such data as a business strategy, beyond the already wide-spread use of 'cookies'.[127] To ensure protection of the rights of potentially affected individuals, the supervisory authorities will thus have to reconcile the application of the underlying rules on a case-by-case basis. This reconciliation might prove especially challenging in light of the fragmented designation of the competent supervisory authority, discussed below, in addition to potential conceptual discrepancies in the rules themselves.[128]

For the purposes of this work, it is warranted to take a specific look at the interplay between the underlying transparency requirements embodied in the aims of explainability as pre-requisites to effective remedies in the digital age. Each of the separate digital legal frameworks exemplifies its own pitfalls in the effective application of the underlying rules concerning transparency in the given algorithmic conduct. For instance, the EU's data protection framework is itself far from homogenous and demands greater procedural and substantive clarity for its effective enforcement.[129] A case in point is the debate on the existence or not of a right to an

[124] DSA, Preamble (10) and (68-69); AI Act Proposal (EP Amendments, 2023), Preamble (12b).
[125] Potentially implicating also other legal rules, such as those under the DSA's companion-legislation – the Digital Markets Act. For the latter interactions with the AI Act and the GDPR see Philipp Hacker, Johann Cordes and Janina Rochon, 'Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond.' Available at: <http://arxiv.org/abs/2212.04997>.
[126] GDPR, Art. 9; DSA, Art. 26(3); AI Act Proposal, Art.10(5).
[127] Arne De Keyser and others, 'Opportunities and Challenges of Using Biometrics for Business: Developing a Research Agenda' (2021) 136 Journal of Business Research 52.
[128] Artur Bogucki and others, 'The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies' (Centre for European Policy Studies 2022) CEPS In-Depth Analysis <https://www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/>.
[129] Eleni Kosta, 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon' [2022] Research Handbook on EU Data Protection Law 68.

explanation under the GDPR,[130] as a key component of safeguards against automated decision-making, governed under a separate provision.[131] One open question in this respect is whether non-compliance with the GDPR transparency obligations enshrined in Article 12 and 13 can be found before the actual data processing takes place that could infringe the rights of an individual.[132] For instance, the provision under AI Act's for the right to explanation states that it shall apply only to the extent to which it is not already provided for under other EU legislation.

Similar conceptual unclarities arise from the AI Act regarding the proposed explicit right to an explanation. As raised above, the latest agreements now include the right of AI subjects to request a clear and meaningful explanation from the deployer of an AI system which was used in a way that affects the AI subject's rights or interests.[133] This explanation should cover the AI system's role in the decision-making process, the primary decision parameters, and the related input data. However, there are exceptions and restrictions in cases where Union or national laws allow them, as long as these exceptions or restrictions respect fundamental rights and freedoms and are necessary and proportionate in a democratic society.

Such intra- and inter-framework conceptual discrepancies will prove decisive and hence problematic for legal certainty in the approaches of supervisory authorities and competent courts to the application of rules in a given context. This situation may have negative implications on the extent of legal protection afforded to the rights of individuals as data subjects, as AI subjects, or as users of online platforms concerned with the legality of certain content. The blending of legal rules is however not unprecedented. However, as we have been witnessing in other contexts, namely in competition law enforcement, an 'integration' of the rules of one legal framework within the enforcement of the rules of another framework might raise issues of competence, legal certainty and undermine respect for the law as a whole.[134] In other words, the conceptual disparities in the interplay between the legal rules of emerging digital *acquis* may ultimately lead to applying different 'metrics' for fundamental

[130] Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143.

[131] GDPR, Art. 22.

[132] See the pending follow up questions to the CJEU in Case C-319/20 *Meta Platforms Ireland Limited* [2022] ECLI:EU:C:2022:322.

[133] AI Act, Chapter 3b Remedies, Art. 68(c).

[134] Orla Lynskey and Francisco Costa-Cabral, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11.

rights protection depending on the type of remedial avenue used in a specific context.[135]

For instance, in a complaint brought before the competent national Digital Services Coordinator concerning the use of sensitive personal data for the DSA and AI Act-prohibited practice of manipulative behavioural advertising, the affected person might also invoke their rights as a data subject under the GDPR, as well as their fundamental rights guaranteed under the CFR. The Digital Service Coordinator might thus either perform a fundamental rights review directly. Alternative, it may be obliged to transfer the claim to the competent supervisory authority, most likely a data protection authority to apply the relevant GDPR rules as *lex specialis*. Where the Digital Service Coordinator assumes jurisdiction over the data protection claims nonetheless as part of the integration of the GDPR in the DSA-enforcement, as has been approved by the CJEU to happen in the competition context,[136] new questions of legal competence to provide effective legal protection to the right affected in this context might arise. Indeed, the designated authority under the DSA might itself not be an authority with sufficient competence, and most importantly, the expertise to handle GDPR or AI Act-related claims.

This fact amplifies the well-established and unsettled phenomenon of infusing other fields, such as competition law, which arguably relies on a neutral method of a purely economic analysis, with data protection and thus fundamental rights considerations. While Lynskey and Costa-Cabral cautiously praised this phenomenon for its potential of nurturing a more holistic approach to fundamental rights protection in the EU's digital policy,[137] the phenomenon does present a complex challenge that should be tackled with the right objectives in mind, precisely to what extent constitutional democracies entrust specialised authorities with quasi-constitutional competence of conducting a review of compliance with fundamental rights. To avoid discussions on the inevitable function creep among the competent supervisory authorities, a holistic approach first and foremost requires fostering clarity in their institutional collaboration.

[135] Simona Demková, 'The EU's Artificial Intelligence Laboratory and Fundamental Rights' <https://papers.ssrn.com/abstract=4566098>.

[136] Case C 252/21 *Meta Platforms v. Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

[137] Lynskey and Costa-Cabral (n 137).

4.3. Fostering Institutional Collaboration

Forging pathways for cooperation between different supervisory authorities becomes crucial to ensuring that individuals can effectively access and exercise their rights while preserving legal certainty in an otherwise complex regulatory environment. Such collaboration should aim to streamline the enforcement of obligations falling upon the different actors, the extent of the underlying and fragmented newly created digital rights. In the meantime, the efforts need to be placed into mitigating the challenges posed by fragmentation, by turning to the competent bodies, including the Commission through its legislative power, as well as to the European Data Protection Supervisor and the European Data Protection Board for their advisory role in providing clear guidelines on the cooperation mechanisms, including through detailed revision of thei procedural rules.

The growth in digital activities and the vast amount of data have pushed supervisory authorities towards a potential 'system overload'.[138] This challenge is particularly evident in the realm of data protection. With ambitious enforcement goals and limited resources, supervisory authorities find themselves compelled to adopt a selective approach, by focusing only on 'strategic cases'.[139] The likely expansion of competences of data protection authorities under the emerging digital legal frameworks further exacerbates this issue, as they struggle to enforce data protection rules effectively. This 'overload' of responsibilities can potentially lead to varying levels of legal protection across Member States, contingent on the resources and capabilities of their respective competent authorities.[140]

The intricate coordination between competition authorities at the Member State level is emblematic of the multifaceted challenges faced in the digital age.[141] *Meta Platforms*

[138] Not only due to the broad definition of personal data as envisaged by Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40.

[139] European Data Protection Board, 'Statement on Enforcement Cooperation, Adopted on 28 April 2022' <https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf>.

[140] Giulia Gentile and Orla Lynskey, (n 77).

[141] EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679. Adopted on 19 September 2023.

v. Bundeskartellamt serves as a case in point.[142] While this legal battle did not concentrate on remedies, it highlighted the complexities of delineating the boundaries of national competition authorities in an increasingly interconnected digital landscape. The question that loomed large was how far these authorities could extend their jurisdiction, even reaching into areas like data protection. The CJEU addressed this overlap by championing institutional collaboration. The Court acknowledged that a national competition authority could assess violations of data protection law as part of its evaluation of compliance with regulations beyond competition law. This approach emphasised the importance of adhering to decisions made by other competent authorities in their respective domains while retaining autonomy to determine the case's outcome within their jurisdiction. The emphasis was on promoting sincere cooperation within the EU, safeguarding its objectives without undermining its unity. The Court focused its attention not on the fungibility of these organisations but on the principle of sincere cooperation within the Union,[143] not to jeopardise the objectives of the Union.[144]

The Commission also seems interested in providing a clearer framework for enforcement, evident with the new constellations for cooperation under the DSA and the new proposal for a regulation clarifying the enforcement procedures of the GDPR.[145] Despite the national differences in terms of resources and scope, this approach aims to avoid potential clashes coming from the increasing fragmentation and overlap of competencies in the internal market. As already demonstrated above, the rules of the AI Act also pose a challenge for the allocation of the competent supervisory authority for its enforcement. In this respect, substantial fragmentation emerges for the specific tasks and responsibilities in the ex-post market surveillance under the AI Act.

Depending on the context of the specific artificial intelligence system's application, the competent supervisory authority in the Member State may vary. This step seems particularly relevant considering the institutional clash between the Irish Data Protection Commission and the European Data Protection Board in the aftermath of

[142] Case C 252/21 *Meta Platforms v. Bundeskartellamt* [2023].

[143] TEU, Art. 4(3).

[144] Case C-518/11 *UPC Nederland* [2013] ECLI:EU:C:2013:709; and Joined Cases C-14/21 and C-15/21 *Sea Watch* [2022] ECLI:EU:C:2022:604.

[145] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, [2023] COM/2023/348 final.

the Meta decision on targeted advertising.[146] The extent of the emerging fragmentation under EU law might be such as to prevent a meaningful harmonisation through the adoption of further procedural rules. In this respect, proposals for centralisation of enforcement, akin to the one recently advanced by Brito-Bastos and Pałka[147] deserve to be seriously considered for the broader context of the Union's digital policy.

This is necessary in view of the fact that in the algorithmic society, collaboration between supervisory authorities and private actors is becoming an integral part of digital governance, including its enforcement, especially within the EU. It is not enough to look at institutional issues without understanding the broader need for a collaborative framework also when it comes to the private sector. This approach marks a significant shift in the relationship between public institutions and online platforms. The EU recognizes that these private entities possess the resources, expertise, and technical capabilities required to effectively address digital challenges. However, they are expected to align their actions with the broader societal values and goals, maintaining a harmonious coexistence with public policy objectives, as underlined by the DSA.

In this evolving landscape, enforcement institutions increasingly rely on the power and influence of tech giants to achieve a more balanced and effective enforcement of public interests. enforcement institutions increasingly rely on tech giants' influence and capabilities to achieve a more balanced and effective enforcement of public interests. The Italian Data Protection authorities' ban on ChatGPT serves as a prime example of not only the potential conflicts that can arise but also the imperative need for collaboration to achieve policy enforcement objectives.[148] The reliance on private actors to enforce remedies introduces the challenge of potentially encroaching on competition and the freedom to conduct business within the internal market. For example, the DSA's obligations apply broadly to online platforms, encompassing not only very large ones. Likewise, the GDPR grants data subjects' rights independently of the data controller's size.

---

[146] European Data Protection Board, 'EDPB Urgent Binding Decision on Processing of Personal Data for Behavioural Advertising by Meta' (1 November 2023) <https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en>.

[147] Filipe Brito Bastos and Przemysław Pałka, 'Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?' [2023] European Constitutional Law Review 1.

[148] Italian Data Protection Authority, decision 9870832 (30 March 2023).

However, there is a risk that private actors may become overwhelmed by managing their internal systems, pushing judicial remedies into the forefront as the only reliable means of redress. This can result in an increased demand for access to judicial remedies, posing challenges to the overall enforcement system. National-level collaboration is further complicated by the diverse enforcement nuances rooted in the constitutional identity of Member States. While the principle of sincere cooperation is a starting point, sectorial harmonization of supervisory authorities' competences and remedies could be a promising path forward, albeit one that raises questions about EU competences. Article 4 TEU underscores the critical importance of this principle while mandating respect for the national identities of Member States, including their political and constitutional structures.

This example underlines that the prevailing trend is not driving enforcement toward centralisation at the European level but rather promoting more effective coordination across competent authorities within Member States. As long as enforcement remains distributed across Member States, institutional conflicts are likely to surface, particularly with the growing fragmentation in European digital policy. Fostering institutional collaboration and addressing these challenges may necessitate a stronger European perspective to better harmonise the relationships between national institutions, even if one the primary challenges is the upgrade of their powers based on EU law.[149] Rather than solely expanding the scope of European digital policy, the emphasis should be on enhancing the coordination of enforcement at both horizontal and vertical levels, as underlined by the new proposal of Regulation on the enforcement of the GDPR.[150]

However, it's essential to be mindful of the potential risks associated with reversing subsidiarity,[151] which could impact national identity and the principle of sincere cooperation, ultimately challenging the EU project and the achievement of policy objectives. National nuances matter and the identity of Member States should be ensured, but not to the point of making the European strategy pointless in terms of enforcement.

[149] Marta Simoncini, Administrative Regulation Beyond the Non-Delegation Doctrine (Hart 2021).
[150] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 COM(2023) 348 final.
[151] Robert Schutze, *European Constitutional Law* (Cambridge University Press 2012); Theodore Konstadinides, 'Constitutional Identity as a Shield and as a Sword: The European Legal Order within the Framework of National Constitutional Settlement' (2011) 13 Cambridge Yearbook of European Legal Studies 195.

5. Conclusion

The examination of the paths paved for access to remedies within the EU's digital laws reveals a delicate balance between the legal design of the remedial procedures under the three frameworks assessed and their practical implementation. Through a comparative analysis of these legislative constellations and their alignment with the constitutional requirements of the right to an effective remedy, this work has scrutinised the evolving landscape within the algorithmic society. By delineating the contours of the right to an effective remedy and navigating the fragmented realm of remedies in EU law, this work has explored the design, nature, and limits of remedies categorised as 'internal complaints,' 'independent supervision,' and 'judicial remedies.' In light of these findings, this paper offered recommendations on interpreting the emerging digital *acquis* so as to ensure optimal safeguarding of the right to an effective remedy. It contributes to the ongoing discourse on the preservation of constitutional fabric of the right to an effective remedy in the ever-evolving digital context, shedding light on potential avenues for closing the existing gaps and reinforcing the existing remedies within the EU's digital policy.