# The Constitutional right to an effective remedy in the digital age: a perspective from Europe

De Gregorio, G.; Demkova, S.; Oirsouw, C. van; Poorter, J. de; Leijten, I.; Schyff, G. van der; ... ; De Visser, M.

# Chapter 10
# The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe


**Giovanni De Gregorio and Simona Demková**

## Contents



**Abstract** The consolidation of the digital age has expanded the demand for justice. The challenges characterising digital relationships have caused European policymakers to reflect on 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 chapter 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, with a particular focus on institutional collaboration across the emerging remedial frameworks.

G. De Gregorio (✉)
Católica Global School of Law, Universidade Católica Portuguesa, Lisbon, Portugal
e-mail: gdegregorio@ucp.pt

S. Demková
Leiden Law School, Europa Institute, Leiden University, Leiden, The Netherlands



C. van Oirsouw et al. (eds.), *European Yearbook of Constitutional Law 2023*, European Yearbook of Constitutional Law 5, https://doi.org/10.1007/978-94-6265-647-5_10

**Keywords** Digital regulation · Effective remedy · European Union · Fundamental rights · Institutional cooperation · Transparency safeguards

## 10.1 Introduction

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

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 was subsequently shaped by the Court of Justice of the European Union (CJEU) from notions of effectiveness and obligations of sincere cooperation of the Member States under Article 19(1) TEU.[3] However, in the EU's emerging algorithmic society, the established constitutional fabric of this right is being stretched by the novel constellations of remedial avenues for the enforcement of individual rights arising 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 Artificial Intelligence Act (AI 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 (DSA). Similarly, the right not to be subject to automated decision-making enshrined in the General Data Protection Regulation (GDPR) 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 the actors involved in the remedial constellation, including private persons, 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 chapter assesses the European regulatory approach to remedies in the EU's digital policy. Through a careful analysis of the emerging remedial constellations, it demonstrates how, despite new remedial systems, the regulatory approach exacerbates the already-existing fragmentation and uncertainty. As

[1] Rabinovich-Einy and Katsh 2017.

[2] See the authors' contributions on the topic: Demková 2023a; De Gregorio 2022.

[3] Aalto et al. 2014.

a result, the effectiveness of remedies in the European algorithmic society firmly depends on the extent to which legislators can realise 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 underscore that there is a thin line between 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 chapter 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 EU's emerging algorithmic society. Therefore, this chapter 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 (Sect. 10.2), before turning to the analysis of the fragmented landscape of remedies in EU digital policy (Sect. 10.3). 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 Sect. 10.4, we highlight the key areas that require further clarification in order to ensure that the emerging digital *acquis* respects the constitutional right to an effective remedy.

## 10.2 The Constitutional 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 of effective judicial protection.[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 its multifaceted nature. Its constitutional fabric stretches beyond the ambit of the Charter's application and covers the broader system of the judicial protection in the EU legal order by determining the EU and Member States' remedial regimes.[8]

The CJEU developed the right to an effective remedy from the notion of effectiveness and the obligation of sincere cooperation of the Member States under Article

[4] Following the requirement reaffirmed by the ECtHR, in *Kudła v. Poland, judgment of 26 October* 2000, Application No. 30210/96, para 157.

[5] Demková and Hofmann 2022, p. 212.

[6] Bonelli et al. 2023, p. 274.

[7] Hofmann and Mihaescu-Evans 2013, p. 73.

[8] Gutman 2019.

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 EU law, the latter requiring also structural guarantees of judicial independence and separation of powers within the Member States. In the latter respect, the current 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]

The Latin maxim *ubi ius, ibi remedium* demands that where there is a right under EU law, there must be a remedy to ensure its enforcement.[11] Beyond the enforcement of individual rights, EU law guarantees 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 an effective remedy entails both demands regarding 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 those 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] However, pursuant to the well-established *Rewe* line of case law,[14] the Court limits this procedural autonomy with the conditions of effectiveness and equivalence. The condition of effectiveness obliges Member States

[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] The Court of Justice of the European Union, Case C-64/16 *Associação Sindical dos Juízes Portugueses,* judgment of 27 February 2018, ECLI:EU:C:2018:117, para 36; The Court of Justice of the European Union, Case C-216/18 PPU *Minister for Justice and Equality v LM,* judgment of 25 July 2018, ECLI:EU:C:2018:586, para 51 and The Court of Justice of the European Union, Case C-72/15 *Rosneft,* judgment of 28 March 2017, ECLI:EU:C:2017:236, para 73.

[11] Demková and Hofmann 2022, p. 212.

[12] The Court of Justice of the European Union, Case C-64/16 *Associação Sindical dos Juízes Portugueses*, judgment of 27 February 2018, paras 35, with reference to Case C-583/11 *Inuit,* judgment of 3 October 2013, ECLI:EU:C:2013:625, paras 91, 94.

[13] Arnull 2020.

[14] The Court of Justice of the European Union, Case 33/76 *Rewe,* judgment of 16 December 1976, ECLI:EU:C:1976:188, para 5; The Court of Justice of the European Union, Case 45/76 *Comet,* judgment of 16 December 1976, ECLI:EU:C:1976:191, para 12; The Court of Justice of the European Union, Case 106/77 *Simmenthal,* judgment of 9 March 1978, ECLI:EU:C:1978:49, paras 21–22; The Court of Justice of the European Union, Case C-213/89 *Factortame,* judgment of 16 June 1990, ECLI:EU:C:1990:257, para 19; The Court of Justice of the European Union, Case C-312/93 *Peterbroeck* judgment of 14 December 1995 ECLI:EU:C:1995:437, para 12; and, more recently, The Court of Justice of the European Union, Case C-619/18 *Commission v. Poland (Independence of the Supreme Court),* judgment of 24 June 2019, ECLI:EU:C:2019:531, para 48 and Case C-64/16 *Associação Sindical dos Juízes Portugueses,* judgment of 27 February 2018, para 34.

to establish the procedures that are compatible with EU 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 the admissibility of complaints and the prospect of effectively hearing a claim and rendering a substantive remedy on the merits.[17]

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 for this limitation of the right to a judicial remedy is legitimate with a view to reducing the additional burden on national courts, as it ultimately contributes to the efficiency of judicial proceedings rather than undermining them.[20] In other words, EU law guarantees a judicial remedy only as the final or ultimate remedy. 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, which are of specific application to public administrations, include the duty of care, the right of access to one's files, the right to be heard and the right to a reasoned decision. The competent authority must exercise due care in its decision-making, demonstrated through a 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

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

[16] The Court of Justice of the European Union, Case C-312/93 *Peterbroeck,* judgment of 14 December 1995, ECLI:EU:C:1995:437, para 14 and The Court of Justice of the European Union, Joined Cases C-430 and 431/93 *Van Schijndel,* judgment of 14 December 1995, ECLI:EU:C:1995:441, para 19.

[17] For a detailed commentary, see Hofmann 2019.

[18] The Court of Justice of the European Union, Joined Cases C-317/08 to C-320/08 *Alassini,* judgment of 18 March 2010, ECLI:EU:C:2010:146, para 63.

[19] The Court of Justice of the European Union, Case C-73/16 *Puškár,* judgment of 27 September 2017, ECLI:EU:C:2017:725.

[20] Ellingsen 2018, p. 1879.

[21] Demková 2023a, pp. 58–59.

[22] Demková and Hofmann 2022.

[23] Mendes 2020.

[24] The Court of Justice of the European Union, Joined Cases C-225/19 and C-226/19 *R.N.N.S., K.A. v Minister van Buitenlandse Zaken*, judgment of 24 November 2020, ECLI:EU:C:2020:951, para 43.

'in a position in which it may carry out the review of the lawfulness' of the decision in question.[25]

The simultaneous application of the remedial rules mentioned above as general principles of EU law means that they bind the authorities even when this is 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 safeguard the quality and integrity of decision-making procedures, allow individuals to know the factual basis for decisions concerning them and enable them to make an informed decision on their chances of obtaining correction or compensation in cases of violation of their rights by seeking remedies. The logic of the prerequisite of good administration to ensuring effective remedies is widely mirrored in the transparency and accountability safeguards enshrined in the EU's emerging digital *acquis*.[27]

However, the algorithmic age demands a more refined remedial framework beyond the availability of judicial remedies. Indeed, the emerging EU digital *acquis* establishes an extensive array of *ex-ante* accountability mechanisms, including impact assessments, continuous reporting and informing duties and 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 in the individual's right to a remedy before the courts. Combinations of administrative and judicial review mechanisms are widespread across EU policy areas. As mentioned earlier, the CJEU clarified in the case of *Puškár*[29] that 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 reinforcing efficiency rather than weakening remedies.

Within this framework, 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 of such internal complaint mechanisms should be subject to close scrutiny through the constitutional lens of the right to an effective remedy as well. The question then arises whether and to what extent the emerging complexity as far

[25] Ibid.

[26] The Court of Justice of the European Union, Case C-166/13 *Mukarubega v. Seine-Saint-Denis*, judgment of 5 November 2014, ECLI:EU:C:2014:2336 paras 43–9; The Court of Justice of the European Union, Case C-521/15 *Spain v Council,* judgment of 20 December 2017, ECLI:EU:C:2017:982, para. 89; The Court of Justice of the European Union, Case C-604/12 *H.N. v. Minister for Justice, Equality and Law Reform, Ireland*, judgment of 8 May2014, ECLI:EU:C:2014:302, para 49.

[27] Demková et al. 2023; Symposium on Safeguarding the Right to Good Administration in the Age of AI. The Digital Constitutionalist of 3 October 2023. Available at: https://digi-con.org/symposium-on-safeguarding-the-right-to-good-administration-in-the-age-of-ai/.

[28] Demková 2023a, p. 55.

[29] The Court of Justice of the European Union, Case C-73/16 *Puškár,* judgment of 27 September 2017, ECLI:EU:C:2017:725.

as the available range of remedial procedures is concerned meets the requirements of the constitutional right to an effective remedy.

## 10.3 Remedial Constellations for the Digital Age

The EU has expanded its regulatory intervention in the digital age. At least three landmark legislative frameworks, set up under the GDPR,[30] the DSA[31] and the AI Act,[32] constitute a milestone in the European approach to governance in the digital age. These legislative frameworks are part of the EU's broader strategy regarding the Digital Single Market,[33] including many additional instruments, such as the Copyright Directive,[34] the amendments to the Audiovisual Media Services Directive[35] and the 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 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 at 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 respect for the constitutional right to an effective remedy.

[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] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act).

[33] European Commission (2015) 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.

[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] Micklitz et al. 2020.

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'.

### *10.3.1 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 through terms of services.[40] Internal complaint-handling systems provide individuals and entities with alternative channels to address violations of their rights without relying on traditional systems of administrative and judicial review. More particularly, internal 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 these are *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 violations 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 subjects' rights, including the possibility to rely on a greater protection of personal data. While the GDPR does not provide for internal complaint mechanisms as a form

[38] Sagy 2011, p. 923.

[39] Radin and Wagner 1999, p. 1295.

[40] Quintais et al. 2023, p. 105792.

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 subjects' 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 in relation to their right to request from the controller rectification, erasure or restrictions regarding the processing of their personal data. Similarly, the controller must inform 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] The centrality of data subjects' rights is also underlined by the expansion of the intermediation to access remedies.[44] Indeed, closely related is the debate about the possible existence of a so-called right to explanation under the GDPR's access to information rights.[45] As discussed below, the AI Act seems to resolve that question by explicitly enshrining the right to explanation under Article 86.

More explicitly, the GDPR provides a mechanism for internal complaints through the role of a data protection officer (DPO),[46] who will be responsible for the internal oversight of compliance with the data protection rules. The DPO can 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 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 the DPO's appointment by the employer.[50]

---

[41] Vrabec 2021.

[42] GDPR, Art. 15–22.

[43] The Court of Justice of the European Union, Case C-553/07 *Rijkeboer*, judgment of 7 May 2009, ECLI:EU:C:2009:293, paras 51–52.

[44] Giannopoulou et al. 2022, p. 316.

[45] See notably, Edwards and Veale 2017; Casey et al. 2019.

[46] GDPR, Article 37.

[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] The Court of Justice of the European Union, Case C-817/19 *Ligue des droits humains v. Conseil des ministres*, judgment of 21 June 2022, ECLI:EU:C:2022:491, para 179.

[49] Ibid, para 180.

[50] GDPR, Art. 38(3), see The Court of Justice of the European Union, Case C-534/20 *Leistritz AG v. LH*, judgment of 22 June 2022, ECLI:EU:C:2022:495, paras 27–28.

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 for violations of their rights by and on online platforms. Compared to its predecessor—the e-Commerce Directive,[51] 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 of robust safeguards to protect the rights and legitimate interests of all parties, particularly their fundamental rights, including the right to an effective remedy.[52]

The DSA also introduces this type of remedies by establishing the obligation to provide internal complaint-handling systems.[53] Importantly, these remedies do not exclude the possibility of resorting to courts and administrative remedies. Under the DSA,[54] contesting decisions of providers of online platforms through internal mechanisms should not detract from an individual's 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'.[55] This approach has expanded the personal scope and 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 their terms and conditions. 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 the precise meaning of these requirements. Instead, the DSA gives discretion to platforms to define their own standards, which can be a point of contention, especially in cases involving political speech. This rule leaves space to online platforms to achieve a decision that defines a fair outcome.[56] 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

[51] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[52] Kuczerawy 2022; Remedying Overremoval: The Three-Tiered Approach of the DSA. Verfassungsblog of 03 November 2022. Available at: https://verfassungsblog.de/remedying-overremoval/.

[53] DSA, Art. 20.

[54] Ibid, Recital (59).

[55] Ibid, Art. 3(b).

[56] Ibid, Recital (58).

complainant's conduct does not warrant the measure taken.[57] 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.[58]

The DSA also introduces a critical safeguard in this process by requiring online platforms not to take decisions on complaints solely based on automated means.[59] Online platforms have to rely on the supervision of qualified staff who will be responsible for internal complaints mechanisms. As a result, artificial intelligence technologies cannot exclusively drive this redress mechanism. This safeguard is critical to ensure that those recipients who have already been subject to an automated decision regarding 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 AI Act advanced by the European Commission in 2021. Instead, the rules of the AI Act should apply without prejudice to other administrative or judicial remedies.[60] Accordingly, as EU 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'.[61] This is because, from its inception, the AI Act was drafted as a product-safety regulation, which builds on demands for developing an internal accountability culture by the AI providers and deployers as the means to ensure compliance with the Act's requirements. The AI Act therefore seems to assume a complementary role in addition to existing EU laws, especially on fundamental rights protection.

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 DPO under the GDPR. Indeed, the AI Act does not envision a figure similar to an AI Officer who would be responsible for the company's compliance with the new rules. Instead, the AI Act aims to create a horizontal compliance culture across the company's chain of responsibilities, enforced through market certification procedures.

Nonetheless, the adopted version of the AI Act includes a rather limited section on remedies.[62] One distinguishing internal remedy that emerges from the AI Act is the right to an explanation of individual decision-making, enshrined in Article 86 of the AI Act. Specifically, 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

[57] Ibid, Art. 20(4).

[58] Ibid, Art. 20(5).

[59] Ibid, Art. 20(6).

[60] AI Act, Preamble (9).

[61] AI Act, Preamble (170).

[62] AI Act, Section 4 'Remedies'. See the discussion in Sect. 10.3.2.

from the deployer on the role of the AI system in the decision-making process and the main elements of the decision.[63]

In addition, pursuant to the general obligations under the AI Act for deployers, providers, and users of high-risk AI systems in individual decision-making,[64] the affected person must be informed that they are subject to the use of such a system. Notwithstanding the usual exception for law enforcement, 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.[65]

As already hinted at above, this provision might put 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,[66] and the underlying requirements of disclosure of the algorithmic logic as well as the significance and the envisaged consequences of automated processing for the data subject. However, the AI Act's right to explanation seems to be formulated in a similarly ambiguous way as the information rights under the GDPR, leaving unresolved the key challenge of identifying 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*,[67] 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 relies heavily on such a probability value to establish, implement, or terminate a contractual relationship with an individual. However, in this respect the Court's interpretation aligns with the object of the GDPR's provision,[68] 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

[63] AI Act, Art. 86(1).

[64] AI Act, Arts 26(11) and 50(1).

[65] AI Act, Art. 50(5).

[66] GDPR, Arts 13(2)(f) and 14(2)(g) and 15(1)(h). For different views on the topic, see Edwards and Veale 2017; Malgieri and Comandé 2017; De Hert and Lazcoz 2021; Radical Rewriting of Article 22 GDPR on Machine Decisions in the AI Era. European Law Blog of 13 October 2021. Available at: https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/.

[67] The Court of Justice of the European Union, Case C-634/21 *Schufa Holding AG,* 2023, ECLI:EU:C:2023:957. See also the analysis of the decision by Palmiotto (2024) 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 of 9 January 2024. Available at: 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/.

[68] 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).

does not seem to provide the necessary guidance for assessing the effects of AI-driven automation on decision-making processes in other contexts.[69]

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.[70]

### *10.3.2 Independent Supervision*

Independent supervision lies at the core of the EU's multilevel accountability system across different policy areas. The vast magnitude and diversity of potential harmful activities in the algorithmic society can affect individual rights and interests and render judicial review not a viable option.[71] Given the demands of the algorithmic age, it is presumed that independent supervision constitutes the cornerstone in the system of remedies in the digital age.

As highlighted above, the CJEU has clarified that rules prescribing an obligation to first exhaust administrative complaint mechanisms before seeking a judicial remedy constitute legitimate limits on the right guaranteed in Article 47 CFR.[72] The Court values administrative review mechanisms to enhance the efficiency of judicial proceedings by reducing the burden where claims can be sufficiently addressed by administrative bodies, provided that these do not place a disproportionate burden, such as costs and time, on the parties.[73]

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 discussed by the Court in its case law.

Regarding the requirement of independence, the CJEU echoes an understanding of the term as referring to 'complete independence',[74] in the form of both formal detachment from other branches of the government so as to prevent both direct and

---

[69] 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.

[70] See Sect. 10.4.1.

[71] Cobbe 2019.

[72] The Court of Justice of the European Union, Case C-73/16 *Puškár*, judgment of 27 September 2017, ECLI:EU:C:2017:253, para 67.

[73] Ibid, para 70 with references to previous case-law of the The Court of Justice of the European Union, Joined Cases C-317/08 to C-320/08 *Alassini and Others*, judgment of 18 March 2010, ECLI:EU:C:2010:146, para 67, and Case C-75/16 *Menini and Rampanelli,* judgment of 14 June 2017, ECLI:EU:C:2017:457, para 61.

[74] See the relevant case-law: namely, The Court of Justice of the European Union, Case C-518/07 *European Commission v Germany*, judgment of 9 March 2010, ECLI:EU:C:2010:125, paras

indirect influence, as well as practical, often discussed as 'functional',[75] or 'operational',[76] independence, evidenced by the supervisory authorities' legal powers 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 a precondition must be provided for by law, respect the essence of the right to an effective remedy and be proportionate to the objectives of the EU's general interest or the need to protect the rights and freedoms of others.[77]

The GDPR provides a general right to lodge a complaint with a supervisory authority.[78] Accordingly, data subjects can access a direct remedy against a violation of their rights that is normally free of charge. Although this remedy cannot lead to the same effects as judicial remedies in terms of ordering a compensation for damages,[79] administrative review plays a role as a critical deterrent for data controllers because of the DPAs' power to impose substantial administrative fines for non-compliance with the GDPR.[80] Indeed, administrative remedies allow data subjects to make their voices heard and thus exercise autonomy over their data and privacy.

The primary limit of administrative supervision lies in the different capacities of data protection authorities across Member States.[81] As in other fields, such as consumer law, the fragmentation of enforcement authorities in the field of data protection could impact how data subjects access remedies across the Member States, given the different institutional setting and resources of their 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,[82] 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 grievance raised and inform the other coordinators as well as the Commission on the resolutions adopted.[83] This right gives users the possibility to

23–25; and The Court of Justice of the European Union Case C-362/14, *Schrems v. Data Protection Commissioner,* judgment of 6 October 2015, ECLI:EU:C:2015:650, para 57.

[75] The Court of Justice of the European Union, Case C 614/10 *European Commission v. Austria,* judgment of 16 October 2012, ECLI:EU:C:2012:631, para 41.

[76] The Court of Justice of the European Union, Case C 288/12 *European Commission v. Hungary*, judgment of 8 April 2014, ECLI:EU:C:2014:237, para 52.

[77] The Court of Justice of the European Union, Joined Cases C-439/14 and C-488/14 *Star Storage and Others,* judgment of 15 September 2016, ECLI:EU:C:2016:688, para 49.

[78] GDPR, Art. 77.

[79] Ibid., Art. 82(6).

[80] But see Lintvedt 2022.

[81] Gentile and Lynskey 2022.

[82] GDPR, Art. 80.

[83] DSA, Art. 53.

notify the supervisory authority that there has been a violation of the DSA, thereby also extending the role of collective remedies.

Besides complaints to the Digital Service Coordinators, the DSA grants the users the possibility to access an out-of-court dispute resolution mechanism.[84] By relying on an entity established by Member States or certified to address disputes as defined by Digital Service Coordinators, access to remedies is still possible for user 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 90 calendar days after the receipt of the complaint.[85] 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 of 180 days.[86]

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.[87] This issue could not only lead to a fragmentation of approaches,[88] 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 through 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 on 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 suggests that this remedy may be less effective, as it still leaves discretion to online platforms not only as regards formally granting access, but also substantially ensuring an effective remedy.

For the AI Act, as explained above, the EU legislators opted for reaffirming the availability of the existing administrative and judicial remedies under EU and national law, also in 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 an administrative complaint mechanism for natural persons by granting them the right to lodge a complaint with a national market surveillance authority where they consider that there has been a breach of the rules of the AI Act.[89]

[84] Ibid., Art. 21(1).
[85] Ibid., Art. 21(4).
[86] Ibid.
[87] Ibid., Art. 21(2).
[88] Wimmers 2021, p. 1.
[89] AI Act, Art. 85.

In such cases, the relevant market surveillance authority must follow the established procedures under the EU Market Surveillance Regulation.[90]

What appears the most problematic in the Act's design is the resulting confusion about its independent supervision, especially where AI systems are used in individual decision-making that also relies on the processing of personal data. In light of the *lex specialis* nature of the European data protection rules,[91] this 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 products on the market.[92] This also entrusts market authorities with the power of hearing complaints from consumers and other private parties, by performing the 'appropriate checks'.[93] There is a lack of understanding about the extent to which these 'appropriate checks', performed with respect to high-risk artificial intelligence products, will be able to effectively address potential fundamental rights complaints.[94]

As a result of this multifaceted design, substantial fragmentation is to be expected regarding the specific tasks and responsibilities as far as the *ex-post* enforcement of the AI Act is concerned. Depending on the context of the use of a specific artificial intelligence system, the competent supervisory authority in the Member State may vary.[95] Exceptions are further acknowledged wherever this is in the interest of cooperation among the supervisory authorities concerned. Similarly, for AI systems used in the context of law enforcement, the supervisory powers should rest with the authority supervising the law enforcement activities.[96]

### *10.3.3 Judicial Remedies*

Judicial remedies represent the ultimate form of remedy in constitutional democracies, including in the EU legal order, as guaranteed under Article 47 CFR. Access to a court is an inherent aspect of the rule of law as an essential component of

[90] 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.

[91] AI Act, Preamble (10).

[92] Only occasionally, the AI Act also engages the national data protection authorities simultaneously with the market surveillance authorities, for instance under obligations for deployers to notify both, and their respective obligation to submit annual reports of such notifications to the Commission, see AI Act, Art 26(6) and (10).

[93] 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.

[94] See Sect. 10.4.3.

[95] AI Act, Art. 74(3) (6) (8) and (9).

[96] AI Act, Art. 74(8).

any democratic system.[97] It gives individuals and organisations the possibility to insist on respect for 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 in different areas from competition to consumer law,[98] and the capacity of court to protect fundamental rights in the digital age.[99]

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 that alleges a violation of the GDPR rules or their rights as data subjects by the data controller.[100] On the other hand, the GDPR further guarantees data subjects the right to seek a judicial remedy against any legally binding decision concerning them that is issued by the independent supervisory authority.[101] The latter scenario occurs when 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 its complaint. This two-fold system of access to judicial remedies underscores the rights-based approach of the GDPR which has as its objective to ensure a high-level protection of the fundamental rights to private life and personal data protection under Articles 7 and 8 CFR.[102]

In *Ligue des droits humains*,[103] the CJEU held that even when the supervisory authority provides only minimum information regarding 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 supporting 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 to a full judicial review, 'which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them'.[104] Essentially, this

[97] See European Court of Human Rights, *Golder v. United Kingdom* judgment of 21 February 1975, Application no. 4451/70, para 34; more recently The Court of Justice of the European Union's Cases C-72/15 *Rosneft*, judgment of 28 March 2017, ECLI:EU:C:2017:236, para 73 and C-216/18 PPU *Minister for Justice and Equality v. LM*, judgment of 25 July 2018, ECLI:EU:C:2018:586, para 51.

[98] Stephenson 2005, p. 93; Sousa Ferro 2022, p. 578.

[99] Pollicino 2023.

[100] GDPR, Art. 78.

[101] GDPR, Art. 79.

[102] Gellert 2020.

[103] The Court of Justice of the European Union, Case C-333/22 *Ligue des droits humains* (Verification by the supervisory authority of data processing), judgment of 16 November 2023, ECLI:EU:C:2023:874.

[104] The Court of Justice of the European Union, Joined Cases C-26/22 and C-64/22 *UF and AB v. Land Hessen*, judgment of 7 December 2023, ECLI:EU:C:2023:958, para 52, reinstating the role of due diligence in the review by the DPA addressed in The Court of Justice of the European Union, Case C-311/18 *Facebook Ireland and Schrems*, judgment of 16 July 2020, ECLI:EU:C:2020:559. See also the analysis of the judgment by Magierska (2024) No, the Data Protection Complaint Is Not a Petition. European Law Blog of 25 January 2024, available at: https://europeanlawblog.eu/2024/01/25/no-the-data-protection-complaint-is-not-a-petition/.

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 ask a not-for-profit body, organisation, or association properly constituted in accordance with the Member States' law, to bring the complaint on their behalf.[105] Furthermore, Member States can 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 the GDPR have been violated due to processing. This is 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 individuals rarely exercise their GDPR rights, including seeking judicial redress for any potential violations, which often incurs high costs.[106] It is therefore unsurprising that most high-level cases concerning the violations of the GDPR originate in complaints brought by civil society organisations.[107] 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.[108] In guaranteeing the right to an effective judicial remedy under Article 47 CFR, the DSA encourages, rather than itself affords, an explicit avenue for accessing the 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.[109] The latter form of judicial remedy in the online environment raises its own challenge due to the limited harmonisation of national legal orders and the territorial limits of national legal decisions concerning online content.[110] 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.[111]

At the very least, the DSA encourages the provision of information regarding redress mechanisms available to both the provider of the intermediary services as

[105] GDPR, Art. 80.

[106] González Fuster et al. 2022.

[107] Including those resulting in landmark CJEU rulings, including the already-mentioned Case C-817/19 *Ligue des droits humains*, with the exception of the 'individual' cases brought by Max Schrems in Case C-362/14 *Schrems v. Data Protection Commissioner* judgment of 6 October 2015, ECLI:EU:C:2015:650, which of course subsequently led him to found one of the most active data protection NGOs in Europe—'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.

[108] DSA, Art. 54.

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

[110] Svantesson 2017a.

[111] European Commission (2023) 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. See the discussion in Sect. 10.4.3.

well as to the users of the services, including about both administrative complaint-handling mechanisms as well as judicial redress. Moreover, the DSA empowers Digital Services Coordinators to develop national tools and guidance regarding national complaint and redress mechanisms to facilitate users' access to such mechanisms.[112] 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 the AI Act does not enshrine an explicit right to seek judicial remedies against the use of AI systems. Although the amendments advanced by the European Parliament included such a right, the trilogue concluded that it was sufficient to acknowledge the judicial remedies already existing under EU law.[113] 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 when they consider their rights and freedoms protected under EU law to be affected.

However, the same 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 AI systems are put to 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,[114] in conjunction with the requirements under the new AI Liability Directive.[115] Ultimately, the access to judicial remedies is likely to be conditioned by the allocation of supervisory competences over AI uses that negatively affect individuals.

## 10.4 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 multifaceted nature. Any discussion regarding efforts for improving 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 of *ex-post* remedies, the constitutional nature of the right to an effective remedy demands that we strive to improve the available mechanisms. This implies both fostering the conceptual clarity

[112] DSA, Recital (39).

[113] AI Act, Section 4.

[114] 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 Bertuzzi (2023) EU Updates Product Liability Regime to Include Software, Artificial Intelligence. Euractiv of 14 December 2023. Available at: https://www.euractiv.com/section/digital/news/eu-updates-product-liability-regime-to-include-software-artificial-intelligence/.

[115] 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.

on the rules that pre-determine effective oversight as well as fostering the institutional collaboration necessary under a fragmented legislative design.

### *10.4.1 Inherent Limits of Ex-post Remedies*

In its case-law in the security context, the CJEU put forward its initial insights regarding the role and exercise of remedies in the algorithmic society.[116] 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.[117] 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'.[118] These insights reaffirm the precondition of sufficient transparency, including through the statement of reasons, for the effectiveness of *ex-post* remedies. 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.[119] While the latter may be too far-fetched a requirement for all types of algorithmic uses, transparency through an *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 necessitate a prior authorisation through a conformity assessment and subsequent certification of any high-risk artificial intelligence systems before they are placed on the EU market. Moreover, the AI Act stipulates obligations for the providers and deployers of artificial intelligence systems to undertake a continuous review and verification of compliance with the AI Act requirements, including through a new

[116] The Court of Justice of the European Union, Joined Cases C-511/18, C-12/18 and C-520/18 *La Quadrature du Net,* judgment of 6 October 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 CJEU, *Ligue des Droits Humains* (2022).

[117] The Court of Justice of the European Union, Case C-817/19 *Ligue des droits humains v. Conseil des ministres*, judgment of 21 June 2022, ECLI:EU:C:2022:49, 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 […].'

[118] Ibid., para 211.

[119] The Court of Justice of the European Union, Case C-817/19 *Ligue des droits humains v. Conseil des ministres*, judgment of 21 June 2022, ECLI:EU:C:2022:491, para 223.

conformity assessment in cases of substantial modifications made to the system.[120] 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 territorial limits.[121] 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. For instance, as stressed in the case *Eva Glawischnig-Piesczek v. Facebook* and in *Google v. CNIL*,[122] national judicial and administrative authorities are limited when issuing orders of removal beyond the EU territorial jurisdiction. Accordingly, the GDPR and the DSA only provide minimum guidance regarding 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.[123] Pursuant to the ruling of the CJEU in *James Elliott*,[124] technical standards trigger only a limited scope of judicial review.[125] In that case, the Court expanded its jurisdiction to review technical standards as acts of private actors, through a teleological interpretation of Article 267 TFEU. However, much remains unclear regarding the review of such instruments, including with respect to the disputes over their copyright protection.[126] Advocate General Medina, in the latter case,[127] reaffirmed 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.'[128] Although this proposition was not explicitly accepted by the Court, Medina argues that there are good reasons to reconsider the nature of

[120] AI Act, Art. 43. 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.

[121] Svantesson 2017b.

[122] The Court of Justice of the European Union, Case C-18/18 Eva Glawischnig-Piesczek v. Facebook Ireland Limited, judgment of 3 October 2019, ECLI:EU:C:2019:821 and Case C-507/17 Google LLC, v. Commission nationale de l'informatique et des libertés (CNIL), judgment of 24 September 2019, ECLI:EU:C:2019:772.

[123] Tovo 2018; Eliantonio and Volpato 2022.

[124] The Court of Justice of the European Union, Case C-613/14 *James Elliott Construction Limited v. Irish Asphalt Limited*, judgment of 27 October 2016, ECLI:EU:C:2016:821.

[125] AI Act, Art. 40.

[126] Judgment of the Court (Grand Chamber) of 5 March 2024, Case C-588/21 P Public.Resource.Org, Inc., Right to Know CLG v. European Commission, ECLI:EU:C:2024:201.

[127] See Opinion of Advocate General Medina in The Court of Justice of the European Union Case C-588/21 P *Public.Resource.Org, Inc., Right to Know CLG v. European Commission, 22 June* 2023, ECLI:EU:C:2023:509.

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

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'.[129] Indeed, this holds even more true with respect to the technical standards for the digital age.[130] While the EU digital *acquis* provides for a 'fallback' option by granting the Commission the power to adopt technical or common specifications via implementing acts in specific cases to protect public interests,[131] the question of the role of standardisation in ensuring protection of the EU's common values, including the protection of fundamental rights remains open and pressing. Lastly, administrative and judicial remedies face a range of not-insignificant practical limits, such as the time and costs of proceedings, as well as the lack of technical expertise in light of the opacity and informational power asymmetry in algorithmic conduct. Furthermore, as stressed above, decisions made by certified dispute resolution bodies under the DSA are not binding on 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 *ex-post* remedies in the digital age becomes somewhat diluted due to the 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 complex. The proliferation of rights and remedies poses a challenge for all the actors involved in the digital accountability infrastructure, from private persons as the users and subjects of digital realm, 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 compliance in light of numerous and inter-related legal obligations, also in light of the supervisory authorities' jurisdictional and other practical limits discussed earlier.

As stressed throughout this chapter, 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. Hence it is of paramount importance to clarify the interplay between the

[129] Ibid., point 21.

[130] 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.

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

various legal frameworks. This clarity is necessary with respect to both the intra- and inter-framework interplay between the explainability obligations regarding a given algorithmic conduct, as preconditions for effective oversight, as well as regarding the provisions on institutional collaboration necessary for coordination among the various remedies.

### *10.4.2 Fostering Clarity in the Interplay of Transparency Requirements*

Effective access to remedies strongly depends on the clarity in the interplay between the regulatory regimes that make up 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 a *lex specialis*.[132] 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.[133] 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.[134] However, research shows an increasing relevance of the use of such data as a business strategy, beyond the already wide-spread use of 'cookies'.[135] 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, as explained above, in addition to potential conceptual discrepancies in the rules themselves.[136]

For the purposes of this chapter, it is warranted to take a specific look at the interplay between the underlying transparency requirements as pre-requisites to effective remedies in the digital age. Each of the separate digital legal frameworks gives rise to 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.[137] A case in point is the debate on

[132] DSA, Preamble (10) and (68-69); AI Act, Preamble (10).

[133] 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 Hacker et al. 2023.

[134] GDPR, Art. 9; DSA, Art. 26(3); AI Act Proposal, Art. 10(5).

[135] De Keyser et al. 2021.

[136] Bogucki et al. 2022.

[137] Kosta 2022.

whether there exists a right to an explanation under the GDPR,[138] as a key component of safeguards against automated decision-making, governed under a separate provision.[139] One open question in this respect is whether non-compliance with the GDPR transparency obligations enshrined in Articles 12 and 13 can be found before the actual data processing takes place that could infringe the rights of an individual.[140] For instance, the right to explanation of the AI Act states that it shall apply only to the extent to which it is not already provided for under other EU legislation.

As raised above, the AI Act now includes 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.[141] 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 EU 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 ambiguities will prove decisive and likely problematic for legal certainty in the approaches of supervisory authorities and competent courts to the application of the relevant rules. The incoherent application of the rules by different Member States' authorities may have negative implications for 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. Indeed, the blending of legal rules is not unprecedented. Yet, as we have witnessed 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.[142] Accordingly, the conceptual disparities in the interplay between the legal rules of emerging digital *acquis* may ultimately lead to applying different 'metrics' for fundamental rights protection depending on the type of remedial avenue used in a specific context.[143]

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 perform a fundamental rights review directly. Alternatively, the Digital Service Coordinator may be obliged to cooperate with or altogether transfer the claim to the competent supervisory authority, most likely a data protection authority,

[138] Casey et al. 2019.

[139] GDPR, Art. 22.

[140] See the pending follow-up questions to The Court of Justice of the European Union in Case C-319/20 *Meta Platforms Ireland Limited,* judgment of 28 April 2022, ECLI:EU:C:2022:322.

[141] AI Act, Art. 86.

[142] Lynskey and Costa-Cabral 2017.

[143] Demková 2023b.

to apply the relevant GDPR rules as a *lex specialis*. Where the Digital Service Coordinator assumes jurisdiction over the data protection claims 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,[144] 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 other fundamental rights considerations. While Lynskey and Costa-Cabral cautiously praised this phenomenon for its potential to nurture a more holistic approach to fundamental rights protection in the EU's digital policy,[145] it also presents a complex challenge that should be tackled with the right objectives in mind, precisely to what extent constitutional democracies entrust specialised authorities with the quasi-constitutional competence of conducting a review to ensure compliance with fundamental rights. To avoid discussions on the inevitable function creep among the competent supervisory authorities, a holistic approach in the application and interpretation of interrelated transparency and other EU digital laws' requirements first and foremost requires fostering clarity in their institutional collaboration.

### *10.4.3 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 incumbent upon the different actors.

The growth in digital activities and the vast amount of data have pushed supervisory authorities towards a potential 'system overload'.[146] 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, often focusing only on 'strategic cases'.[147] The likely expansion of competences of data protection authorities under the emerging digital *acquis*

[144] The Court of Justice of the European Union, Case C 252/21 *Meta Platforms v. Bundeskartellamt,* judgment of 4 July 2023, ECLI:EU:C:2023:537.

[145] Lynskey and Costa-Cabral 2017.

[146] Not only due to the broad definition of personal data as envisaged by Purtova 2018.

[147] 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.

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.[148]

The intricate coordination between competition authorities at the Member State level is emblematic of the multifaceted challenges faced in the digital age.[149] *Meta Platforms v. Bundeskartellamt* serves as a case in point.[150] While this legal battle did not focus on remedies, it highlighted the complexities of delineating the boundaries of national competition authorities in an increasingly interconnected digital landscape. The question was how far these authorities could extend their jurisdiction, even reaching into areas like data protection. The CJEU addressed this overlap by framing the basics of 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 stresses 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. Emphasis was placed on promoting sincere cooperation within the EU, thus 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 EU,[151] not to jeopardise the objectives of the EU.[152]

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.[153] Despite 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 earlier, 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.

---

[148] Gentile and Lynskey 2022.

[149] 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.

[150] The Court of Justice of the European Union, Case C 252/21 *Meta Platforms v. Bundeskartellamt,* judgment of 4 July 2023, ECLI:EU:C:2023:537.

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

[152] The Court of Justice of the European Union, Case C-518/11 *UPC Nederland BV v. Gemeente Hilversum,* judgment of 7 November 2013, ECLI:EU:C:2013:709; and Joined Cases C-14/21 and C-15/21 *Sea Watch,* judgment of 1 August 2022, ECLI:EU:C:2022:604.

[153] 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.

Depending on the context of the specific artificial intelligence system's application, the competent supervisory authority in the Member States 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 the *Meta* decision on targeted advertising.[154] 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 the centralisation of enforcement, akin to that recently advanced by Brito-Bastos and Pałka deserve to be seriously considered for the broader context of the EU's digital policy.[155]

Yet, 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. As evidenced in this chapter, the remedial constellations under EU digital *acquis* mark a significant shift in the relationship between public institutions and online platforms. The EU recognises 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, for a harmonious coexistence with public policy objectives, as underlined by the DSA.

In this evolving landscape, 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 both the potential conflicts that can arise as well as the need for collaboration to ensure fundamental rights protection.[156] 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, and not only to very large platforms. Likewise, the GDPR grants data subjects' rights independently of the data controller's size.

However, there is a risk that private actors may become overwhelmed by managing their internal complaint-handling 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, placing a further burden on 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 harmonisation of supervisory authorities' competences and remedies could be a promising path forward, albeit one

[154] 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.

[155] Brito Bastos and Pałka 2023.

[156] Italian Data Protection Authority, decision 9870832 (30 March 2023). See also Italian Data Protection Authority, ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI (29 January 2024). https://garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020#english.

that raises questions about EU competences. Article 4(2) TEU underscores the critical importance of this principle while mandating respect for the national identities of Member States, including their political and constitutional structures.[157]

This example underlines that the prevailing trend is not driving enforcement toward centralisation at the European level, but rather to 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. Fostering institutional collaboration and addressing these challenges may necessitate a stronger European perspective to better harmonise the relationships between national institutions, even if the primary challenge is the upgrade of their powers based on EU law.[158] Rather than solely expanding their tasks and competences, the emphasis should be on enhancing the coordination of enforcement at both the horizontal and vertical levels, as attempted by the new proposal of a Regulation on the enforcement of the GDPR.[159]

However, it is essential to be mindful of the potential risks associated with reversing subsidiarity,[160] 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.

## 10.5 Conclusion

An examination of the avenues for individuals to access an effective remedy across 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 chapter 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 chapter has explored the design, nature, and limits of remedies categorised as 'internal complaints', 'independent supervision', and 'judicial remedies'. In light of these findings, this chapter offered recommendations on interpreting the emerging digital *acquis* so as to ensure optimal safeguards for the right to an effective remedy. It contributes to the ongoing discourse on the preservation of the constitutional fabric of the right to an effective remedy in the ever-evolving

[157] See also Timmermans 2022.

[158] Simoncini 2021.

[159] 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.

[160] Schütze 2012 and Konstadinides 2011.

digital context, shedding light on potential avenues for closing the existing gaps and reinforcing the existing remedies within the EU's digital policy.

**Acknowledgement** Open access to this publication is supported by a Leiden University Starter Grant funded by the Dutch Ministry of Education, Culture and Science for the project: 'The EU's Human-Centered Digital Transformation' led by Simona Demková.

## References

Aalto P et al (2014) Article 47—Right to an Effective Remedy and to a Fair Trial. In: Peers S, Hervey T, Kenner J, Ward A (eds) The EU Charter of Fundamental Rights: A Commentary. Hart Publishing, Oxford. pp. 1196–1275

Arnull A (2020) Article 47 CFR and National Procedural Autonomy. European Law Review 45:681–693

Bertuzzi L (2023) EU Updates Product Liability Regime to Include Software, Artificial Intelligence. Euractiv of 14 December 2023. Available at: https://www.euractiv.com/section/digital/news/eu-updates-product-liability-regime-to-include-software-artificial-intelligence/

Bogucki A, Engler A, Perarnaud C, Renda A (2022) The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies. In: Centre for European Policy Studies (eds) CEPS In-Depth Analysis. Available at: https://www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/

Bonelli M, Eliantonio M, Gentile G (2023) Conclusions. In: Bonelli M, Eliantonio M, Gentile G (eds) Article 47 of the EU Charter and Effective Judicial Protection: Volume 2: The National Courts' Perspectives. Hart Publishing, Oxford

Brito Bastos F, Pałka P (2023) Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity? European Constitutional Law Review 19(3):1–31

Casey B, Farhangi A, Vogl R (2019) Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise. Berkeley Technology Law Journal 34:143–188

Cobbe J (2019) Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making. Legal Studies 39(4):636–655

De Gregorio G (2022) Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press, Cambridge

De Hert P, Lazcoz G (2021) Radical rewriting of Article 22 GDPR on machine decisions in the AI era. Eur. Law Blog. https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/ (accessed 11.30.21)

De Keyser A, Bart Y, Gu X, Liu S Q, Robinson S G, Kannan P K (2021) Opportunities and Challenges of Using Biometrics for Business: Developing a Research Agenda. Journal of Business Research 136(C):52–62

Demková S (2023a) 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, Cheltenham

Demková S (2023b) The EU's Artificial Intelligence Laboratory and Fundamental Rights. In: Fink M (ed) (2024) Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies' (forthcoming). Cambridge University Press, Cambridge. Available at: https://papers.ssrn.com/abstract=4566098

Demková S, Hofmann H C H (2022) General Principles of Procedural Justice. In: Ziegler K S, Neuvonen P J, Moreno-Lax V (eds) Research Handbook on General Principles of EU Law: Constructing Legal Orders in Europe. Edward Elgar Publishing, Cheltenham. pp. 209–226

Demková S, Fink M, Gentile G (2023) Symposium on Safeguarding the Right to Good Administration in the Age of AI. The Digital Constitutionalist. Available at: https://digi-con.org/symposium-on-safeguarding-the-right-to-good-administration-in-the-age-of-ai/

Edwards L, Veale M (2017) Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For. Duke Law & Technology Review 16:18–84

Eliantonio M, Volpato A (2022) The European System of Harmonised Standards. Legal Opinion for ECOS (Social Science Research Network 2022) SSRN Scholarly Paper 4055292 Available at: https://papers.ssrn.com/abstract=4055292

Ellingsen H K (2018) Effective Judicial Protection of Individual Data Protection Rights: Puškár. Common Market Law Review 55:1879–1898

Gellert R (2020) 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: Gellert R (ed) The Risk-Based Approach to Data Protection. Oxford University Press, Oxford

Gentile G, Lynskey O (2022) Deficient by Design? The Transnational Enforcement of the GDPR. International and Comparative Law Quarterly 71(4):799–830

Giannopoulou A, Ausloos J, Delacroix S, Janssen H (2022) Intermediating data rights exercises: the role of legal mandates. International Data Privacy Law 12(4):316–331

González Fuster G et al (2022) 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. Available at: https://www.accessnow.org/cms/assets/uploads/2022/06/Complaint-study-Final-version-before-design-June-15.pdf

Gutman K (2019) 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? German Law Journal 20(6):884–903

Hacker P, Cordes J, Rochon J (2023) Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond. European Journal of Risk Regulation 1:38

Hofmann H C H (2019) The Right to an Effective Remedy and to a Fair Trial - Article 47 of the Charter and the Member States. In: Peers S, Harvey T, Ward A (eds) The EU Charter of Fundamental Rights: A Commentary, 2nd edn. Hart Publishing, Oxford

Hofmann H C H, Mihaescu-Evans B C (2013) The Relation between the Charter's Fundamental Rights and the Unwritten General Principles of EU Law: Good Administration as the Test Case. European Constitutional Law Review 9(1):73–101

Konstadinides T (2011) Constitutional Identity as a Shield and as a Sword: The European Legal Order within the Framework of National Constitutional Settlement. Cambridge Yearbook of European Legal Studies 13:195–218

Kosta E (2022) A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon. In: Kosta E, Leenes R, Kamara I (eds) Research Handbook on EU Data Protection Law. Edward Elgar Publishing, Cheltenham. pp. 68–90

Kuczerawy A (2022) Remedying Overremoval: The Three-Tiered Approach of the DSA. Verfassungsblog of 03 November 2022. Available at: https://verfassungsblog.de/remedying-overremoval/

Lintvedt M N (2022) Putting a Price on Data Protection Infringement. International Data Privacy Law 12(1):1–15

Lynskey O, Costa-Cabral F (2017) Family Ties: The Intersection between Data Protection and Competition in EU Law. Common Market Law Review 54(1):11–50

Magierska M (2024) No, the Data Protection Complaint Is Not a Petition. European Law Blog of 25 January 2024. Available at: https://europeanlawblog.eu/2024/01/25/no-the-data-protection-complaint-is-not-a-petition/

Malgieri G, Comandé G (2017) Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. International Data Privacy Law 7(3):243–265

Mendes J (2020) The Foundations of the Duty to Give Reasons and a Normative Reconstruction. In: Fisher E, King J, Young A (eds) The Foundations and Future of Public Law: Essays in Honor of Paul Craig. Oxford University Press, Oxford. pp
Micklitz H-W, Pollicino O, Reichman A, Simoncini A, Sartor G, De Gregorio G (eds) (2020) Constitutional Challenges in the Algorithmic Society. Cambridge University Press, Cambridge
Palmiotto F (2024) 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 of 9 January 2024. Available at: 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/
Podszun R (2022) Private Enforcement and Gatekeeper Regulation: Strengthening the Rights of Private Parties in the Digital Markets Act. Journal of European Competition Law & Practice 13:4–254
Pollicino O (2023) Judicial Protection of Fundamental Rights Online. A Road Towards Digital Constitutionalism? Hart Publishing, Oxford
Purtova N (2018) The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Law, Innovation and Technology 10(1):40–81
Quintais J P, De Gregorio G, Magalhães J C (2023) How Platforms Govern Users' Copyright-Protected Content: Exploring the Power of Private Ordering and Its Implications. Computer Law & Security Review 48
Rabinovich-Einy O, Katsh E (2017) Digital Justice Technology and the Internet of Disputes. Oxford University Press, Oxford
Radin M J, Wagner R P (1999) The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace. Chicago-Kent Law Review 73(4):1295–1317
Sagy T (2011) What's So Private about Private Ordering? Law & Society Review 45(4):923-954
Schütze R (2012) European Constitutional Law. Cambridge University Press, Cambridge
Simoncini M (2021) Administrative Regulation Beyond the Non-delegation Doctrine: A Study on EU Agencies. Hart Publishing, Oxford
Sousa Ferro M (2022) Consumer Antitrust Private Enforcement in Europe. Journal of European Competition Law & Practice 13(8):578–593
Stephenson M C (2005) Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies. Virginia Law Review 91(1):93–173
Svantesson D J B (2017a) Scope of (Remedial) Jurisdiction. In: Solving the Internet Jurisdiction Puzzle. Oxford University Press, Oxford. pp 171–190
Svantesson D J B (2017b) The Tyranny of Territoriality. In: Solving the Internet Jurisdiction Puzzle. Oxford University Press, Oxford. pp 13–56
Timmermans C (2022) Mediating conflicts between national identities and EU law: The potential of Article 4(2) TEU. Common Market Law Review 59(SI):75–86
Tovo C (2018) Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law. Common Market Law Review 55(4):1187–1216
Vrabec H U (2021) Data Subject Rights under the GDPR. Oxford University Press, Oxford
Wimmers J (2021) The Out-of-court dispute settlement mechanism in the Digital Services Act—A disservice to its own goals. Journal of Intellectual Property, Information Technology and E-Commerce Law 12(5):381–401

## Other Documents

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