The (In)Effectiveness of EU Data Protection: A Rejoinder

Giulia Gentile

Abstract: The emergence of a highly privatised digital environment driven by data has triggered a regulatory response in the EU built on public law tools, such as fundamental rights. The EU fundamental right to data protection has had a central role in scrutinising the conduct of tech companies within the EU and beyond. The application of this fundamental right has followed an expansive trajectory, aimed at offering effective and complete protection, to use the words of the European Court of Justice. Yet the fundamental right-driven enforcement of EU data protection rules has been heavily criticised, and not without reason. Among the several critiques, it has been observed that the breadth of data protection entails enforcement challenges, while the proceduralisation of this right *de facto* disguises the preservation of a business model in favour of digital actors. This chapter offers a rejoinder to these critiques by reflecting on and contextualising the criticisms of data protection's effectiveness against the background of the human rights' crisis. As the chapter demonstrates, several challengers against EU data protection rules mirror a broader critical movement against human rights. Hence, while many stances against data protection are worthy of consideration, scholars and regulators should not lose sight of the gains and protections afforded by data protection as a fundamental right. As a matter of fact, human rights remain one of the most effective tools to counteract imbalances of powers due to their iterative engagement governance, especially in the digital society.

A. Introduction

Data structures and underpins digital society. We can trace data in almost every daily activity carried out by individuals and public bodies: statistical

All the links have been accessed on 9 September 2024.

evidence and data are likely to underlie an increasing number of policies;[1] the study of patients' health and lifestyle is conducted through data analysis;[2] administrative decisions increasingly rely on data,[3] and so on. The emergence of a pervasive data-driven society was favoured by a private tech power, which exploited the structures of the digital environment in its favour. EU institutions[4] and States[5] have counteracted those imbalances of digital power though law, and especially the recognition of fundamental rights such as that to data protection. The application of fundamental entitlements in the digital environment was innovative, to a certain extent, as it affected private parties such as online platforms. It further signalled the advancement of public value considerations in the highly privatised digital environment, built on the exploitation of data. The advancement of constitutional guarantees to the digital environment has been captured under the concept of 'digital constitutionalism'.[6]

---

1 Md Altab Hossin et al 'Big Data-Driven Public Policy Decisions: Transformation Toward Smart Governance' (2023) 13(4) Sage Open, https://doi.org/10.1177/21582440231215123; Michela Arnaboldi and Giovanni Azzone, 'Data science in the design of public policies: dispelling the obscurity in matching policy demand and data offer' (2020) 6 Heliyon https://www.cell.com/action/showPdf?pii=S2405-8440%2820%2931144-0.

2 Richard Brown et al, 'Collecting and sharing self-generated health and lifestyle data: Understanding barriers for people living with long-term health conditions - a survey study' (2022) 8 Digit Health 1; see also the UK National Health System approach to data collection and data sets, available at https://digital.nhs.uk/data-and-information/data-collections-and-data-sets#:~:text=Our%20data%20collections%20cover%20many,authorities%20and%20independent%2Dsector%20organisations.&text=Our%20national%20data%20sets%20collect,areas%20of%20health%20and%20care.

3 See in the UK context the UK Department for Science, Innovation and Technology, 'Ethics, Transparency and Accountability Framework for Automated Decision-Making' 29 November 2023, available at https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making; Ulrik B.U. Roehl, 'Automated decision-making and good administration: Views from inside the government machinery' (2023) 40(4) Government Information Quarterly 101864.

4 See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281 (Directive 95/46).

5 See DLA Piper 'Data Protection Laws of the World' https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2=DE.

6 Edoardo Celeste, 'Digital constitutionalism: a new systematic theorisation' (2019) 33(1) International Review of Law, Computers & Technology 76; Giovanni De Gregorio, 'The rise of digital constitutionalism in the European Union' (2021) 19(1) International Journal of Constitutional Law 41; Nicolas Suzor, 'Digital constitutionalism: Using the

Enshrined in Article 8 of the EU Charter and Article 16 TFEU, the fundamental right to data protection played a significant role in the EU digital constitutionalism. Data protection rules, introduced in the EU with Directive 95/46, were designed to address several challenges stemming from the emergence of data power, such as the regulation of personal data processing and the need to ensure harmonised rules on personal data transfers in the internal market.[7] Data protection cases like *Google Spain*[8] or the *Schrems* saga[9] demonstrated the power of fundamental rights, and especially data protection, in constraining digital power.[10] The latest iteration of data protection rules, the General Data Protection Regulation (GDPR), is a globally leading framework that has acted as a blueprint for other data protection laws across the world.[11] The GDPR has introduced several innovations, including detailed rules on remedies and enforcement[12] for the transnational enforcement of data protection rights.[13]

As an emanation of a fundamental right, by nature open-ended and amenable to judicial interpretation, data protection rules have been interpreted under a constitutional approach. Examples of the expansive fundamental-right interpretation of EU data protection rules concern the concept of personal data[14] and data processing,[15] the narrow reading of the house-

rule of law to evaluate the legitimacy of governance by platforms' (2018) 4(3) Social Media + Society 1.

7 See e.g. recitals 2 and 3 of Directive 95/46.

8 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317.

9 See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (*Schrems I*) EU:C:2015:650; Case C-311/18 *Facebook Ireland and Schrems (Schrems II)* EU:C:2020:559.

10 Also across the Atlantic the application of fundamental rights guarantees regarded digital matters such as freedom of speech and indecent or obscene material (Reno v American Civil Liberties Union 521 US 844 (1997) and privacy (ACLU v Clapper 785 F3d 787 (2n Cir 2015).

11 Annegret Bendiek and Isabella Stuerzer 'The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate' (2023) 20(5) Digital Society.

12 See Chapter 8 GDPR.

13 See Chapter 7 GDPR.

14 See Case C-434/16 *Nowak* EU:C:2017:582.

15 See Case C-101/01 *Bodil Lindqvist* EU:C:2003:596.

hold exemption,[16] and the joint liability regime for controllers.[17] Through the door of the GDPR, Big Tech's data power has been subject to scrutiny.

Yet the EU data protection rules have also been heavily criticised. The very features that have supported the broad application of the data protection framework, and, namely, its expansive scope (driven by the fundamental right approach), have been the target of several critiques. For example, authors have remarked that data protection rules apply to everything[18] and everyone,[19] and that they replicate market dynamics hidden behind a fundamental right narrative.[20] Laws that are excessively broad encounter enforcement problems and may not be effective. Lynskey has argued that the GDPR rules aspire to completeness, but cannot be effective.[21] In turn, it has been observed, a cumbersome framework may limit innovation and market freedoms.[22] Hence a paradox has materialised: while the fundamental right nature of data protection, and the consequent broad application of rules, were deemed as necessary by regulators to address the imbalances of power in the digital environment, they were also identified as its very weaknesses that undermine the effectiveness of data protection rules.

The effectiveness challenge for EU data protection rules is a critique that underlies the adoption of the Data Protection and Digital Information Bill (DPDIB) in the UK[23] – now defunct – in the aftermath of the withdrawal from the EU and the loss of the EU Charter from the UK legal order. Striking but perhaps unsurprising features of this framework were the very

16 See Case C-212/13 *Ryneš* EU:C:2014:2428.

17 See Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388.

18 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.

19 Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297.

20 See the discussion on consent and legitimate interest as a ground for lawful processing, Midas Nouwens et al 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems April 2020 1 https://doi.org/10.1145/3313831.3376321.

21 Lynskey (n 19).

22 Ryan Preston, 'Stifling Innovation: How Global Data Protection Regulation Trends Inhibit the Growth of Healthcare Research and Start-Ups' (2022) 37 Emory Int'L L Rev 135.

23 See UK Government, 'Data Protection and Digital Information Bill', available at https://bills.parliament.uk/bills/3430.

scarce references to fundamental rights' protection,[24] and the de-valuation of data protection to a set of procedural rules rather than a fundamental entitlement in its own right. Hence, while it favoured market interests and innovation, the Bill sought to abandon the ability to protect personal data as a matter of fundamental rights protection.[25]

These criticisms and policy developments test the conceptual boundaries of data protection and question its effectiveness as a source of fundamental protection. Has the fundamental right to data protection failed to demonstrate its value?[26] This paper argues that those critiques need to be contextualised in the broader crises of human rights.[27] As will be demonstrated, the contestation raised against data protection as a framework – and especially as a fundamental right – essentially reflect a critical movement against human rights.[28] In recent years, whether human rights are an effective mechanism to protect individuals and public values in our society has been questioned.[29] Accordingly, critiques to the effectiveness of data protection should be filtered to avoid falling prey to narratives that are essentially anti-human rights. While human rights have been criticised for

24 One of the consequences of Brexit has been the loss of the EU Charter of Fundamental Rights and the fundamental right to data protection granted thereunder. Accordingly, the UK Government has sought to seize the opportunity for innovation and increased competitiveness by revising data protection rules, and introducing the DPDIB. If adopted, this new framework could significantly transform the ability of individuals to protect their personal data.

25 This approach was evidently in stark contrast with the European Union context which instead recognises acknowledges the value of data protection as a fundamental right.

26 Orla Lynskey 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63(3) ICLQ 569; Maria Tzanou 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right' (2013) 3(2) International Data Privacy Law 88.

27 While the terminology 'human right' is typically used in the context of international law, 'fundamental rights' is generally employed in a European context.

28 Andrew Fagan, 'The Subject of Human Rights: from the Unencumbered Self to the Relational Self' (2024) The Nordic Journal of Human Rights 215; Kiyoteru Tsutsui 'Justice Lost! The Failure of International Human Rights Law To Matter Where Needed Most' (2007) 44 Journal of Peace Research 407; Oren Gross '"Once More Unto Breach": the Systemic Failure of Applying the European Convention on Human Rights to Entrenched Emergencies' (1998) 23 Yale Journal of International Law 436; Eric Posner, 'The Case Against Human Rights' 4 December 2014, The Guardian https://www.theguardian.com/news/2014/dec/04/-sp-case-against-human-rights; David Kennedy, 'The International Human Rights Movement: Part of the Problem?' (2002) 15 Harvard Human Rights Journal 101.

29 See also Eric Posner, *The Twilight of Human Rights* (OUP, 2013).

reinforcing neo-liberal dynamics and power structures, they nonetheless remain a legal tool that allows accountability and the imposition of positive and negative obligations on duty-bearers. In so doing, they have an equalising and protective function, insofar as they support the scrutiny of behaviours of parties in positions of power. According to de Búrca, the value of human rights stems from the 'iterative engagement'[30] governance they engender.

Similarly, personal data protection as a fundamental right has three features that make it particularly apt to respond to the complexities of the digital society. These are protectiveness, dialogue and a high degree of universality. Combined, these give rise to a governance structure that enhances scrutiny over the use of data by private and public bodies. Such scrutiny, although imperfect and certainly requiring improvement, allows the exercise of control over the behaviour of data entities enjoying a position of power over data subjects. The ability to scrutinise the conduct of data processors and controllers fosters an iterative approach to the regulation of the digital environment, which in turn stimulates reflections on the power dynamics of specific fields of law. By highlighting the value of data protection as a fundamental right, the chapter does not intend to entirely dismiss the criticisms raised against data protection. Many critiques are valuable and seek to foster better regulation of personal data. Yet, when rethinking data protection, sight should not be lost of the positive side of the story of the fundamental right to data protection: the data feudalism that permeates the digital environment can be successfully rebalanced through legal tools such as fundamental rights.

The paper proceeds as follows. First, it introduces the challenges of digital constitutionalism; then it explains the foundations of data protection rules in the EU legal order. Subsequently, the chapter critically analyses the fitness of data protection in the context of digital constitutionalism in light of the various critiques advanced in the literature. It does so by highlighting how the effectiveness crisis of data protection mirrors the deeper contestation experienced by human rights in recent decades. Conclusions will follow.

30 Grainne de Búrca, *Reframing Human Rights in a Turbulent Era*, (OUP, 2021) at 10.

B. The challenges of digital society and digital constitutionalism

Digital constitutionalism is a label used for an emerging regulatory phenomenon in the digital environment. Namely, digital constitutionalism seeks to capture the use of the law, and especially public law, to restrain the power of private digital entities that have permeated society in an increasing fashion. While there is a plurality of understandings of digital constitutionalism, they tend to converge on two tenets. First, the proliferation and strengthening of private digital actors has created power imbalances in the digital word. Second, due to their implications in the real world, these 'digital-power-imbalances' demanded regulatory tools, the law appearing as central to restrain power and tackle abuses perpetrated by private actors in the digital field. Both these dynamics speak to the introduction of public law guarantees in the online space. The prominent role of fundamental rights' protection in the EU digital regulation articulates one of the aspects of 'EU digital constitutionalism'. Digital constitutionalism can therefore be conceptualised as a legal response to the establishment of a 'digital society' governed by power dynamics and relationships with novel features linked to the structures of the internet and technology.[31] The use of public law in the context of digital constitutionalism essentially addresses three challenges stemming from the digital society.

First, with the emergence of the digital society and the rise of online platforms, digital private entities have benefitted from a prominent position and power vis-à-vis individuals.[32] Thanks to their ability to govern the structures, including access and enjoyment of digital services, the architects of the digital world were able to claim 'regulatory' authority in their space.[33] In so doing, these bodies have shaped the online digital world, as well as the freedoms and legal entitlements of users and players engaging with these technologies. For instance, social media platforms became, willingly or not,

31 See Tomi Dufva and Mikko Dufva, 'Grasping the Future of the digital society' (2019) 107 Futures 17; Vitaly V. Martynov, 'Information Technology as the Basis for Transformation into a Digital Society and Industry 5.0' available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8928305&casa_token=lb2s_fNfG-MAAAAA:MfzCoQEL8Eo9ElPgfz935n97JNYk3CvrLqUGs1WlbvdxTl4OhueA_EnUYYd7wdyuUelTOPfOXQHc&tag=1.

32 For a general discussion see Martin Moore and Damian Tambini (eds) *Digital Dominance: The Power of Google, Amazon, Facebook and Apple* (OUP, 2018).

33 See the discussion on 'Code is Law' initiated by Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

responsible of the freedom of speech of their users, as well as their ability to access information services or education.[34]

In turn, the dominant position of the architects of the digital society was amplified by a twofold externality. First, the merging of market power with digital power. Companies, such as Amazon, Facebook and Google, have de facto monopolies in the digital market.[35] And because of their dominant position in the markets, they can also more easily gather big data through their users. Such incredible amount of data also allows these entities to know more and more about their users, and ultimately, affect their free choice and fundamental rights.[36] Second, the informational gap and a-symmetries in favour of tech companies. Both regulators and individuals have for long been in a position of relative ignorance and seldom disregard concerning the digital world and its implications on society: the ignorance of others was power for digital actors. As described De Gregorio and Radu,[37] the *laissez-faire* attitude of the regulators has strengthened private digital power. Digital constitutionalism seeks to rebalance this imbalance on the online space.

A second challenge that digital constitutionalism grapples with is that of reconciling fundamental rights protection with other public interests, and, especially, the economic structures and rules of the (digital) market. As a matter of fact, it is complex to align market interests with fundamental rights protection: one of the two should at least partially give in. Because of the public interests identified in economic and market policies, as well as the limitations that are intrinsic to fundamental rights vis-à-vis public interests, fundamental rights have often been treated as secunda ratio to

34 Kate Klonick, 'The new governors: The people, rules, and processes governing online speech' (2017) 131 Harv. L. Rev. 131, 1598; see the liberal dimension of digital constitutionalism described by Francisco de Abreu Duarte et al, 'Perspectives on Digital Constitutionalism' in Bartosz Brozek et al (eds.), *Handbook on Law and Technology* (Edward Elgar, forthcoming) https://ssrn.com/abstract=4508600.

35 Emilio Calvano and Michele Polo 'Market power, competition and innovation in digital markets: A survey' (2021) 54 *Information Economics and Policy* 100853.

36 Nathalie de Marcellis-Warin et al., 'Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools' (2022) 2 AI Ethics 259.

37 Giovanni De Gregorio and Roxana Radu, 'Digital constitutionalism in the new era of Internet governance' (2022) 30(1) International Journal of Law and Information Technology 68.

the achievement of market goals and objectives.[38] At the same time, the opposite result involving the prevalence of fundamental rights over market objectives has been criticised both by companies and regulators as a possible constraint over innovation and the competitiveness.[39]

Seen from another perspective, the tension between individual and collective rights and values underpins the developments of digital constitutionalism. Focusing on data protection, the dichotomy between individual and collective interests emerges powerfully. Indeed, the protection of personal data might, in certain circumstances, hinder the protection of other fundamental rights, such as that to freedom of expression.[40] In addition, the perception of data protection breaches might change depending on whether we look at individual or collective implications. For instance, it has been argued that individual violations do not resonate as much as collective, systematic abuses of data protection rules, due to the scale of societal impacts and harms.[41] In this context, because of the broad applicability of data protection rules and the need to adjudicate these tensions, courts have been at the forefront of the digital constitutionalist transformation. The image that results from the jurisprudence of the cyberspace is one of polycentricity, with several complex dynamics and interests coming to the fore.

A third challenge explored by digital constitutionalism is the transnational enforcement of the law and especially of constitutional rules in the digital society.[42] Because of the transnational nature of several databases, social media and AI technologies, questions arise on the legal frameworks that apply to the digital environment and data.[43] From the perspective of digital constitutionalism, what is of interest is how to solve normative conflicts and the clashes of different conceptions of public law and fundamental

38 Síofra O'Leary, 'Balancing Rights in a Digital Age' (2018) 59 Irish Jurist 59 https://www.jstor.org/stable/26431267.

39 See Cat Zakrewsky 'Tech companies spent almost $70 million lobbying Washington in 2021 as Congress sought to rein in their power' (2022) The Washington Post https://www.washingtonpost.com/technology/2022/01/21/tech-lobbying-in-washington/.

40 David Erdos, 'Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation' (2021) 40 Yearbook of European Law 398–430, https://doi.org/10.1093/yel/yeab004.

41 Omri Ben-Shahar, 'Data Pollution' (2019) 11 Journal of Legal Analysis 104.

42 Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet* (Hart, 2021).

43 Ibid.

entitlement. And this becomes particularly evident when considering the protection of privacy broadly understood and the freedom of expression in the US and in the EU.[44] Hence, digital constitutionalism also reflects on the migration of values and principles that influence digital regulation and enforcement.

All in all, the three challenges of power asymmetries and imbalances, balancing of rights and interests and migration and development of fundamental rights and values are not extraordinary to the digital constitutionalism *per se*. Yet the legal issues emerging from the digital environment stretch the common understandings of rights' entitlements and protections, and push the boundaries of the law to tackle novel questions, actors and tools. It is in light of this background that we should consider the effectiveness of data protection as a fundamental rights framework in tackling the challenges of digital constitutionalism.

C. European Data Protection Rules: objectives and tools

Data protection rules have been established at the EU level since 1995 with the adoption of Directive 95/46 that set out the blueprint for personal data protection across the Member States.[45] The introduction of EU data protection rules was premised on two practical issues. First, the increasing overproduction of and overreliance on data, which can be used to identify, profile, exclude and manipulate individuals.[46] The need to protect individuals from abuses deriving from the exploitation of their personal information accordingly emerged. In this context, the fundamental right to privacy was put under strain and exposed to novel tests, due to the invisibility of privacy breaches through data (ab)use and the technologies used for the processing of personal data. A secondary challenge was of internal market's matrix, being the need to ensure harmonised protection for personal data in the context of cross-border transfers of information and data across the European Union.[47] In this sense, EU data protection rules were borne out at the intersection between fundamental rights and internal market objectives.

44 Ibid.
45 Orla Lynskey, *The Foundations of Data Protection* (OUP, 2015).
46 See Recital 4 Directive 95/46.
47 See Recital 3 Directive 95/46.

The fundamental right dimension of data protection emerged before the entry into force of the EU Charter.[48]

Since 2018, the Directive has been replaced by the GDPR, which has strengthened some of the tenets of data protection rules in Europe. The GDPR has essentially bolstered the fundamental right dimension of data protection while detailing procedural rules for the processing of personal data and cooperation among data protection authorities.[49] Indeed, the EU Charter of fundamental rights has officially introduced a fundamental right to data protection under EU law.[50] It has been already discussed that data protection has a specific role that cannot be fully replicated under the right to privacy.[51] Data protection and privacy are two connected rights, but the former adds value to the latter.[52] Namely, data protection allows individuals to control the use and security of their data. Other theories on the role of data protection as a fundamental right have focused on its separate and instrumental nature in relation to privacy.[53] Another aspect that data protection rules expand compared to privacy protection is the ability to offer enhanced protection to sensitive data.[54] The fundamental right to data protection, supported by its procedural framework, empowers data subjects to monitor the information relating to them. In parallel, data controllers and processors have a series of obligations to ensure personal data lawfully. Hence, data protection is the EU fundamental digital right *par excellence*. The data protection as a fundamental right presents several features shared with other EU fundamental rights, such as labour rights[55] or consumer protection.[56]

48 See *Lindqvist* (n 15) in which the Court of Justice linked data protection to the fundamental right to privacy, para 79.

49 Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 ICLQ 799.

50 However, see Convention 108.

51 Lynskey, 'The added value of data protection', (2014) 63(3) ICLQ 569.

52 Lynskey (n 26).

53 Tzanou (n 26).

54 Ibid.

55 See among others Article 31 of the EU Charter of Fundamental Rights, as interpreted in the *Bauer* case, C-569/16 EU:C:2018:871.

56 See Article 38 of the EU Charter of Fundamental Rights.

Regulated and proceduralised

The fundamental right to data protection in the EU is highly regulated through secondary measures, coupled with several opinions issued by the European Data Protection Board (EDPB) and, previously, Article 29.[57] Hence, courts in the Member States and at EU level can rely on a plethora of guidance documents. Moreover, in addition to the EU rules and procedures, national procedural rules also play a role in the enforcement of data protection rules. In so doing, the protection of personal data is harmonised but leaves space for the peculiarities of national systems. For instance, the variance of procedural rules involved in the enforcement of data protection can hinder the effective and equal enforcement of data protection rights across the EU.[58]

Breadth

Data protection is a broad fundamental right *ratione personae*, *materiae*, and *loci*. Anyone whose personal data[59] is affected can invoke the protection of personal data protection under Article 8 of the EU Charter. But in addition to a broad personal scope, the fundamental right to personal data protection also has a broad material scope. Data protection rules cover all areas of human activities that involve personal data processing.[60] The consequence of this framework is that only in few instances – carefully crafted under the GDPR – is it possible for Member States to exclude the reach of data protection rules, an example being national security.[61] The broad scope *ratione materiae* and *loci* is further expanded by the horizontality of data protection. Through the more detailed rules of the GDPR, the fundamental right to data protection imposes very specific procedural obligations and duties to entities (be they private or public) processing personal data.

But beyond the broad personal and material scope of application of the GDPR, it is also well-settled that data protection rules apply also beyond

57 See Lynskey (n 19).
58 Gentile and Lynskey (n 49).
59 See Articles 2 and 3 GDPR.
60 The concept of data processing is very broad, too. See Lynskey (2023) and Opinion of AG Bobek in Case C-245/20 *X and Z v Autoriteit Persoonsgegevens* EU:C:2021:822.
61 See Article 2 GDPR. However, cfr with Article 23 GDPR.

the borders of the European Union, as demonstrated by the *Schrems* saga and as clearly established in the GDPR.[62] Data protection rules also bind third countries and their operators so long as they have been recognised as providing an equivalent protection to the EU in the field of data protection or so long as in any event individuals are sending are consenting for their personal data to be processed in the territory of that third country. The broad scope of application of data protection may be deemed as unique. However, several judicial decisions from the EU Courts and scholars have indicated that the EU Charter can also apply extra-territorially, so long as EU law is applicable.[63] Therefore, data protection rules are a byproduct of EU law and its international reach.

Weight

Another feature of data protection is that it is a very 'heavy' fundamental right in the context of balancing carried by the CJEU. The scale has often tilted in favour of data protection against the freedom of expression[64] or the ability of individuals to carry out journalistic activities.[65] Personal data as a fundamental right is subject to the rules of the EU Charter which require, for instance, that the essence of personal data protection is always respected, while instead its periphery can be derogated.[66] The violation of the essence of data protection remarkably led to the annulment of the Safe Harbour decision in the *Schrems I* case.[67] In that case, the CJEU granted comprehensive protection to data protection, and connected fundamental rights, over other interests, such as trade and data flow to third countries. The importance of data protection in balancing exercises is shared with

62 See Article 3 GDPR.
63 Eva Kassoti and Ramses A. Wessel, 'The EU's Duty to Respect Human Rights Abroad; The Extraterritorial Applicability of the EU Charter and Due Diligence Considerations' (2020) available at https://www.asser.nl/media/680298/cleer_020-02_web_final.pdf.
64 See *Google Spain* (n 8).
65 See Case C–345/17 *Buidvids*. EU:C:2019:122.
66 See Takis Tridimas and Giulia Gentile 'The Essence of Rights: An Unreliable Boundary?' (2019) GLJ 794.
67 See *Schrems I* (n 9).

other EU fundamental rights, such as the right to an effective remedy protected under Article 47 of the EU Charter.[68]

Enforcement framework

In addition to the enforcement that individuals can claim through individual remedies, public-oriented enforcement structure also underpins the framework of data protection rules in the EU, relying on the role of Data Protection Authorities (or DPAs). These bodies are the watchdogs of GDPR-application across Europe and are granted a crucial guarantee of being independent.[69] The independence of the DPAs is of the essence according to the relevant provisions that construe the meaning of data protection rules.[70] The independent nature of DPAs is instrumental both to ensure the freedom of those bodies from public powers, but also to effectively carry out activities that may require quasi-adjudicatory powers, such as the management of complaints under the GDPR.

Moreover, data protection is a peculiar fundamental right because of the tension that exists between transnational and national enforcement. While data can be produced and stored locally, data tends to travel beyond borders. Let us consider the possibility to access websites in any territory of the European Union, or the ability of data subjects to process their personal data beyond national borders. To regulate those instances, the GDPR provides rules on the transnational enforcement of data protection through the Cooperation and Consistency mechanisms.[71] The ability to enforce the GDPR in a transnational context is crucial to ensure data subjects' control over their personal data, even though the personal data moves across borders. At the same time, the tension between national and transnational enforcement of data protection rules has brought to the fore several questions and doubts on the reach of those rules, as well as the com-

68 See Case C-64/16 *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* EU:C:2018:117, and the Polish judges saga, including cases such as C-*619/18 European Commission v Republic of Poland* EU:C:2019:531.

69 See Article 16 TFEU and Article 8 EU Charter of Fundamental Rights.

70 Case C-518/07 *Commission v Germany* EU:C:2010:125 para 23; Case C-614/10 *Commission v Austria* EU:C:2012:631 para 37; Case C-288/12 *European Commission v Hungary* EU:C:2014:237 para 51.

71 See Gentile and Lynskey (n 50).

petence of different bodies involved in the enforcement of this framework, such as the various DPAs of the member states or the EU institutions.[72]

Procedural legitimacy

Finally, data protection is a highly proceduralised fundamental right. The EU data protection framework lays down procedural duties imposed on data processors and controllers.[73] The existence of these procedures between the data subject, the data processor and the data controller influences the ways in which data protection as a fundamental right can be exercised. Examples are provided by the procedural rights that individuals enjoy vis-à-vis data processors and controllers, such as the right to access their data, the right to object to personal data processing, or the right to receive an explanation of the processing by the personal data processor. The presence of procedural elements in the GDPR framework points to a high level of input legitimacy, whereby data subjects, controllers and processors can engage in participatory procedures.[74]

Having set out the content and the peculiar features of data protection, the next section introduces the critiques to the effectiveness of data protection as a fundamental right and a framework more generally.

D. Critiquing EU data protection rules

There are essentially three arguments that underlie the contestation against EU data protection rules.

The first criticism is that data protection rules are the law of everything and everyone,[75] and for this reason their effective enforcement cannot be achieved. The argument suggests that the broad scope of data protection undermines its effectiveness. This is because the aspirations of the EU data protection framework cannot reasonably be met in light of the various constraints on enforcement bodies, time, and more generally resources

72 Ibid.
73 See Chapter 4 GDPR.
74 Alexander I Ruder, Neal D Woods, 'Procedural Fairness and the Legitimacy of Agency Rulemaking' (2020) 30(3), Journal of Public Administration Research and Theory 400, https://doi.org/10.1093/jopart/muz017.
75 See above.

for individuals.[76] A broad scope of application entails that individuals can invoke data protection rules in virtually all circumstances in which a form of personal information and data processing is involved. The GDPR's focus on individual remedies, while providing only limited collective, public remedies,[77] only exacerbates the inability to effectively enforce data protection. As a result, the burden of the data protection rules' enforcement lies on the shoulders of individuals who might not have the time or ability to consistently monitor how their personal data has been processed and whether this has been done lawfully.[78] In parallel to the focus on individual remedies, mention should be made of the complexity for GDPR public enforcement. The GDPR's broad scope also affects the ability of administrators to enforce data protection rules. Constraints such as budget, and a lack of staff limit the power of DPAs to proceed with all data protection complaints – and sometimes even to deal with them in an effective manner. Seen from the companies' perspective, the GDPR is also too cumbersome for companies that are overwhelmed with procedural requirements, and those mechanisms may not lead to meaningful protection. As discussed by Lynskey, data protection cannot be both effective and complete.[79]

There is also a second, powerful argument. The weight that Luxembourg courts have afforded the right to data protection in context of balancing has seldom obscured other fundamental rights and interests.[80] The oversized nature of data protection has established a form of constitutionalism that situates data protection at the peak of the hierarchy of values.[81] Hence, those who support freedom of expression as a higher value for democratic society compared to privacy and personal data processing will see an enemy in data protection.[82] This line of argument also underpins a feminist critique to EU data protection rules. Legal scholars have observed that the GDPR system is Eurocentric and tends to colonise the approach to fundamental

76 Lynskey (n 19).
77 See Article 80 GDPR.
78 See Gentile and Lynskey (n 50).
79 Lynskey (n 19).
80 David Erdos 'European Union Data Protection and Media Expression: Fundamentally Off Balance' (2016) 65(1) International and Comparative Law Quarterly 139.
81 Pollicino (n 42) at 137 and ff.
82 Erdos (n 80).

rights balancing in third countries[83] favoured by the extra-territorial reach of the GDPR.[84] The reach of personal data protection rules as developed in Europe leads to a form of balkanization of the fundamental rights landscape that compresses other perspectives on fundamental rights balancing across the globe.[85]

A third critique against data protection rules is the so-called business model critique,[86] which contradicts, to a certain extent, the previous critique. Several scholars have observed that the data protection framework reproduces innovation and market considerations linked to the digital markets' structures and actors, without providing meaningful protection to data subjects. Accordingly, while the framework provides an appearance of protective aspiration, in reality, it supports tech companies by subjecting the protection of personal data to the existing business structures.[87] An example on point is the impact assessment requirement developed under the GDPR.[88] As observed in literature, this procedure leads to limited, if not minimal, protection of personal data because of its formulaic dimension not necessarily conducive of enhanced protection for individuals.[89] The business model critique has also emerged as a result of judicial ex-post rationalisation of rules in light of Big Tech's business models. The *GC* case decided by the European Court of Justice is an instance of such ex-post rationalisation of data protection rules in light of the Big Tech's approach to data processing.[90]

Ultimately, these criticisms question the protection that individuals can derive from the current EU data protection framework, which is excessively broad in scope, tends to take over other fundamental rights when in conflict and is Eurocentric, and fosters a business model that may not be conducive of effective protection. Such critiques become even more press-

83 Jens T. Theilen, et al 'Feminist data protection: an introduction' (2021) 10(4) Internet Policy Review DOI: 10.14763/2021.4.1609. https://policyreview.info/articles/analysis/feminist-data-protection-introduction.

84 Ibid.

85 Pollicino, (n 42) at 137 and ff.

86 https://www.sciencedirect.com/science/article/pii/S0007681322001288.

87 Lynskey (n 19) at 324.

88 See Article 35 GDPR.

89 Eyup Kun, 'Questioning The Effectiveness of The Data Protectıon Impact Assessment under the GDPR In Time of COVID-19 Crisis' (June 30, 2020). Koronavirüs Döneminde Güncel Hukuki Meseleler Sempozyumu Bildiri Tam Metin Kitabı (İbn Haldun Üniversitesi Yayınları) 743, available at https://ssrn.com/abstract=4002566.

90 Lynskey (n 19) at 336.

ing when considering the legal systemic challenges of the digital society, including the rebalancing of individual protections vis-à-vis Big Tech companies, the reconciliation of fundamental rights and other interests, and the transnational enforcement of laws in the digital environment. Are EU data protection rules and the data protection fundamental-right-dimension developed in the EU an effective, resilient mechanism for the systemic challenges of the digital society?

As the following section will illustrate, the identified criticisms certainly have value and should not be taken lightly. Yet the controversy around data protection appears to have hijacked by several narratives that concern the field of fundamental rights more in general. Such lines of arguments have been subject to scrutiny and scholars have offered reflections to nuance them, thus shedding light on the value of human rights.[91] Hence, when considering those lines of arguments in the field of data protection, we should equally filter those claims, or else risk of falling prey of anti-human rights narratives. Only more nuanced critiques of data protection, as for any other fundamental right, can permit us to identify what to reform, what to maintain, and what to eliminate, especially in light of the advancement of the digital society and its systemic challenges.

E. The crisis of data protection as a human rights crisis: a rejoinder

The critiques of data protection both as a framework and as a fundamental right should be contextualised in the broader debate which has emerged in recent years *against* human rights. As a matter of fact, the criticisms raised against data protection mirror a broader crisis experienced by human rights.

Human rights (also called as 'fundamental rights' in a European context) are not an entirely recent idea or project. Woodiwiss[92] observed that Locke was among the first thinkers to argue that a series of entitlements belong to humans as such, regardless of the presence of a social contract under a natural law approach. These entitlements are grounded in freedom, equali-

91 de Búrca (n 30), Gráinne de Burca, 'Human Rights Experimentalism' (2015) Max Weber Lecture https://cadmus.eui.eu/bitstream/handle/1814/38110/MWP_LS_DeBurca_2015_02.pdf?sequence=1&isAllowed=y.

92 Anthony Woodiwiss *Human Rights*, (Routledge 2005) at 36.

ty and independence.[93] But since Locke, human rights have undergone a series of transformations and evolutions in conjunction with revolutions and wars. As a result of the World War II, human rights have entered the common language and the political agenda of various jurisdictions and international organisations. Authors have spoken of a new form of constitutionalism that draws from the expansive, protective power of human rights.[94] After a period of expansion in the 20th century, the criticisms have started arising. Prominent scholars such as Posner,[95] Moyn[96] and Hopgood[97] have advanced powerful arguments against the effectiveness of human rights. We can identify at least six criticisms that are currently questioning the value and effectiveness of fundamental rights, which, to a certain extent, also permeate the critiques of data protection explored above.

The first critique directed to human rights is a form of general contestation. Several authors also argued that human rights are too broad and ubiquitous, and for this reason, they are highly contested.[98] Human rights are abstract, aspirational, and searching a soul, using the language of Baxi.[99] This is akin to the 'law of everything' critique for data protection.

A second critique advanced against human rights is encapsulated by the expression 'money over values'.[100] The repeated financial crises that have affected Europe but also the rest of the world have put strain on the protection of fundamental rights. As a result, governments are pressured to deliver fundamental rights protections in a context of limited public resources. Under the current financial constraints, fundamental rights have become secondary to public budget considerations, thus fostering the idea

93 Ibid.

94 Richard Bellamy, 'Political constitutionalism and the Human Rights Act', (2011) 9(1) International Journal of Constitutional Law 86.

95 Eric Posner, *The Twilight of Human Rights* (OUP, 2013).

96 Samuel Moyn, *Not Enough: Human Rights in an Unequal World* (Harvard, 2019).

97 Stephen Hopgood, *The Endtimes of Human Rights* (Cornell University Press, 2015).

98 See literature cited at n 28.

99 Upendra Baxi 'Critiquing Rights: The Politics of Identity and Difference' in Aakash Singh Rathore and Alex Cistelecan Wronging Rights? Philosophical Challenges for Human Rights (Routledge, 2011), 61.

100 Rana S. Gautam, *Human Rights Practices During Financial Crises* (Springer, 2019), Emma Luce Scali, *Sovereign Debt and Socio-Economic Rights Beyond Crisis: The Neoliberalisation of International Law* (CUP, 2022).

that human rights ultimately entrench neo-liberalism in society.[101] As a matter of fact, the enforcement of fundamental rights can become particularly expensive when it comes to data protection rules. For instance, the enforcement requires several actions before courts or before administrations with a very complex technical dimension: initiating and advancing these actions is costly and demands financial resources. This criticism is linked to the 'law of everything' critiques discussed above insofar as it acknowledges that effective enforcement of data protection rules, whose scope of application is ever-expanding, depends on sufficient public resources, and as such cannot be fully achieved.

A third root of the crisis of human rights is legal complexity and polycentricity.[102] Fundamental rights are increasingly operating in a polycentric environment, where they may conflict not only with other general interests, but also with other fundamental rights. As a result, creating a hierarchy of values and of fundamental rights within legal orders has become highly contested and complex. This critique echoes the argument according to which during balancing exercises data protection is likely to overtake other values and objectives worthy of protection.

A fourth critique that has affected fundamental rights and that also shapes the crisis of EU data protection results from generalisation of failures. Specific failures of human rights have been generalised and weaponised against human rights. Because of these failings, the effectiveness of human rights as tools to protect the vulnerable has been questioned.[103] The same line of argument has emerged in the field of EU data protection. The limits to the enforcement of data protection rights emerged in cases like *GC*,[104] in which the CJEU has de facto allowed the processing of sensitive data against the wording of the GDPR, or the partial effectiveness of impact assessment under the GDPR[105] should not entail completely dismissing the value of data protection.

101 Samuel Moyn, 'A Powerless Companion: Human Rights In The Age Of Neoliberalism' (2014) 77(4) Law and Contemporary Problems, 147–169. http://www.jstor.org/stable/24244651; Susan Marks, 'Human Rights and Root Causes' (2011) 74(1) The Modern Law Review 57.

102 Jeff King 'Polycentricity' in Jeff King, *Judging Social Rights* (CUP, 2021) 189-210.

103 Fagan (n 28), Posner (n 28).

104 Case C-136/17 *GC* EU:C:2019:773.

105 Nóra Ni Loideain and Rachel Adams, 'From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments' (2020) 36 Computer Law & Security Review 105366.

Last but not, human rights have been contested as a legal domain that has been progressively colonised by private powers. In other words, the public nature of those entitlements has been challenged by subjecting their realisation to private entities choices. For instance, the application of human rights such as the right to freedom of expression or due process by private bodies could lead to a form of responsive regulation that undermines the public nature of data protection rules.[106] Similarly, the application of data protection by private bodies bears the same risk of infusing private, tech-driven values in an area governed by public values, such as data protection. This criticism correlates to the business model critique explored above.

Clearly, human rights, including data protection, are under the spotlight. Yet this paper submits that human rights, and especially data protection, remain one of the most appropriate tools to face digital society's challenges. Human rights are essential for the protection of fundamental entitlements and new vulnerabilities precisely thanks to their expansive scope and their adaptability. Hence, fundamental rights can offer protections that may be crucial in the context of the digital society and could ultimately rebalance the imbalances of the digital society. Fundamental rights also offer a dialectic tool for legal reasoning in reconciling conflicting rights and interests, by providing special protection to certain values deemed essential in societies governed by the rule of law.[107] They also have universal aspirations that make them prone to transnational enforcement, although various constitutional systems may resist their advancement.[108]

Similarly, the EU fundamental right to data protection has *protective*, *dialogic* and *universal* aspirations that make it particularly suited to deal with the challenges of the digital society. The following sections illustrates the effectiveness of the fundamental rights' governance, before critically discussing the features of data protection as a fundamental right and their effectiveness.

106 See Kate Klonick 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) 129(8) Yale Law Journal 2418.

107 See Robert Alexy 'Constitutional Rights, Balancing and Rationality' (2003) Ratio Juris 16(2) 131; Takis Tridimas 'Wreaking the wrongs: Balancing Rights and the Public Interest in the EU Way' (2023) 29(2) Columbia Journal of European Law 185.

108 See the approach of the US to privacy and data protection, for a discussion see Pollicino (n 43) at 137 and ff.

F. The fundamental right governance of EU Data Protection

Protective

The EU fundamental right to data protection seeks to protect data subjects. It does so by empowering individuals to control their data and imposing obligations on data processors and controllers. The independence of DPAs is an essential feature highlighting the protective nature of EU data protection rules.[109] Fundamentally, the enforcement structure of the GDPR is in alignment with its protective intentions. That protecting role for the EU data protection framework should be preserved: in light of the advancement of the digital society, it would be short-sighted to limit the reach of data protection rules, insofar as they ensure the ability to scrutinise the conducts of tech companies relying on personal data. The varying perceptions of the harms caused by data protection violations should not be used to undermine its importance. A useful parallel is the right to vote or the right to paid leave: while not everyone may decide to exercise those fundamental entitlements, it does not mean that their centrality for democracy is lost.

The above observations do not aim to underestimate the challenges surrounding data protection rules. For instance, it has been extensively discussed how the consent model enshrined in the GDPR could lead to paradoxical situations where individuals cannot effectively control their data processing and become victims of dark patterns.[110] The very protective rationale for EU data protection rules would seem defeated. Another challenge to the protectiveness of data protection rules is the entanglement of those rules with economic considerations. Personal data is used by several entities as part of their business models. To empower data subjects, Malgieri and Custers advocated for the right to know the economic value of personal data, with the hope of increased awareness and empowerment concerning the fundamental right to data protection.[111] At the same time, it has been observed that subjecting the exercise of a fundamental right such

109 See Article 16 TFEU and Article 8 EU Charter.

110 Midas Nouwens et al, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) CHI Conference on Human Factors in Computing Systems available at https://arxiv.org/pdf/2001.02479; Cristine Utz et al, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (2019) CCS proceedings, available at https://dl.acm.org/doi/pdf/10.1145/3319535.3354212.

111 Gianclaudio Malgieri and Bart Custers 'Pricing privacy–the right to know the value of your personal data' (2018) 34(2) Computer Law & Security Review 289.

as that to data protection to the payment of a fee commodifies that entitlement and diminish its protectiveness. The EDPB observed that the 'Pay or Okay' model recently proposed by Meta, according to which that platform could charge users a fee to avoid the processing of their data, hinders the protective aspirations of data protection as a fundamental right.[112]

Regulators and enforcers have a crucial role in determining the content and application of data protection rules, and should be cautious not to water down its protective ambitions. The importance of data protection as a protective framework is also a matter of education and sensibility towards the increasing risks and threats posed by the digital society. The more the public becomes aware of the exploitation engendered by the digital environment, the more it can, and likely will action the protections afforded by the fundamental right to data protection in the EU.

Dialogue

The presence of procedural duties and rights under the GDPR enhances the input legitimacy of the framework. Through procedures, the parties involved in the enforcement of data protection rules can exchange their views and opinions in a dialogue aimed at identifying the correct interpretation of EU data protection rules, while also ensuring the achievement of data protection as a public value. Examples of iterative governance fostered by the GDPR are the Consistency and the Cooperation mechanisms that govern the transnational enforcement of data protection rules.[113] Through these procedures, DPAs, the EDPB, data processors and controllers and (although to a more limited extent) data subjects can participate in shaping the governance of personal data protection.

While the scrutiny entailed by the GDPR procedures may not be fully complete or effective,[114] it nonetheless opens a gate in the curtain of the tech companies' world and potential abuses of personal information for their own purposes. Such iterative dynamics, which involve national and European bodies as a form of experimental governance which, according

112 EDPB 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' 17 April 2024 https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

113 See Chapter 7 GDPR, for instance.

114 Gentile and Lynskey (n 50).

to de Búrca,[115] is of the essence for the success of fundamental rights. The presence of various actors and channels of enforcement for data protection entitlements may not be a guarantee for effectiveness in the short term, but certainly stimulates critical considerations and ultimately long-term reflections on the enforcement strategies to adopt in the field. This becomes evident when considering the recent reforms and proposals[116] adopted by the EU Commission and the EDPB, which have both participated in a complex institutional negotiation for improving the future of GDPR, and supported by the public and academic discourses. Seen from another perspective, such a dialogue preserves the ability of individuals and public bodies to ensure the scrutiny of the behaviour of tech companies processing personal data. Such dialogic structures also allow market operators and companies acting as processors and controllers to input their views in the enforcement of EU data protection rules.

But frameworks imbued with procedural legitimacy considerations are not entirely free of risks. A crucial limitation is the potential undermining of *substantive* justice: the existence of procedures that seek to foster dialogue and input from all the parties involved in a dispute may not necessarily reach the *fairest* outcomes.[117] This is all the more likely in situations of imbalance of power that emerge in the digital environment, whereby individuals may not enjoy the same access to legal resources and advice as powerful tech corporations. These observations do not wish to dismiss the value of procedural legitimacy. On the contrary, it should be recalled that procedural justice is also interested in equality of arms, and thus has an equalising power.[118] In other words, the achievement of procedural justice and ultimately legitimacy lies in the ability of regulators and legal frameworks to address the disadvantages experienced by parties involved in a dispute to make their views heard. The procedures governing the enforce-

115 de Búrca, (n 30) at 10.

116 European Commission 'Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases' 4 July 2023 available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609. This proposal has received the green light from the Council, see Council of the EU 'Data protection: Council agrees position on GDPR enforcement rules' 13 June 2024 available at https://www.consilium.europa.eu/en/press/press-releases/2024/06/13/data-protection-council-agrees-position-on-gdpr-enforcement-rules/.

117 See David Thacher 'The Limits of Procedural Justice' in David Weisburd and Anthony Braga (eds.) *Police Innovation: Contrasting Perspectives* (CUP, 2019).

118 Cathérine Van de Graaf 'Procedural fairness: Between human rights law and social psychology' (2021) 39(1) Netherlands Quarterly of Human Rights 11.

ment of the EU fundamental right to data protection have the ambition and the ability to attain the demands of procedural justice, including equality of arms, so long as the regulators and enforcers of data protection address the imbalances of resources that may emerge from the digital environment.[119] Other fundamental rights, such as that to effective remedies and a fair trial included in the EU Charter, have already demonstrated their potential for strengthening the data protection as a fundamental entitlement.[120]

Universality

The EU fundamental right to data protection has a broad scope of application, even beyond the boundaries of the EU.[121] It also relies on several procedures and rules on international transfers, as well as the Cooperation and Consistency mechanisms that apply in the context of the transnational enforcement of the GDPR. Mention should be also made of the Council of Europe's Conventions 108 and 108+, both enhancing the broad application of data protection also beyond EU borders.[122] While these documents do not affect the application of EU rules on data protection, they strengthen the case of the universal aspiration of EU data protection as a fundamental right. Such universality facilitates transnational enforcement strategies that are necessary in the borderless digital environment. While contested as a form of colonialism and balkanisation,[123] the fundamental nature of EU data protection provides nonetheless protection beyond the EU borders to EU citizens invoking that right. In the increasingly inter-connected and globalised digital society, the universal ambition of data protection provides data subjects with entitlements and defences vis-à-vis instances of abuses of their personal data.

In light of the above discussion, the EU fundamental right to data protection offers a solid battleground for the risks and challenges of the digital society that digital constitutionalism seeks to address. Hence, its importance as an EU fundamental right should not be underestimated or undermined in future reform attempts. It would be short-sighted to lower

119 Gentile and Lynskey (n 50) at 808 and ff.
120 *Schrems I* and *II* (n 9).
121 See the *Schrems* cases (n 9) and Articles 2 and 3 GDPR.
122 See Council of Europe, 'Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data' (2018).
123 Pollicino (n 42) at 130 and ff.

the protection offered by this fundamental right, especially in light of the advancement of the digital society and its intrinsic threats, including the rapid developments of artificial intelligence. Rather, such a fundamental right has already played and will continue to play a fundamental role in ensuring that technological developments maintain a human centric perspective aimed at protecting individual values such as autonomy and dignity. A fundamental right approach to the digital environment, such as that offered by data protection in the EU appears a first promising step in regulating the digital environment and its risks. Data protection, like all other fundamental rights, should not simply dismissed due to selected failures or inefficiencies. There is a value in fundamental rights that cannot be easily replicated by other legal instruments. All in all, the current fundamental right approach to EU data protection seems appropriate to face the challenges of the digital society and digital constitutionalism.

G. Conclusion

The digital society, with its challenges, is here to stay. The EU´s fundamental right to data protection has been applied by EU and national institutions in several crucial cases that have shaped the regulation of the digital environment in the EU and beyond. At the same time, data protection is one of the most contested legal frameworks and fundamental rights in the EU. It has been challenged by private parties, academics and institutions alike. Many of these criticisms contain elements of truth and valid observations that should be considered by regulators in future reforms of EU data protection rules. Yet this chapter has attempted to demonstrate that many of the criticisms affecting EU data of mirror more a more general contestation towards human right. Hence, the critiques towards data protection as a fundamental right and a framework more in general should be filtered. Only nuanced criticisms of data protection as a fundamental right, also taking into account its advantages to address the challenges of the digital society, can lead to a more strategic and better rethinking of that fundamental entitlement. The chapter has illustrated that the EU fundamental right to data protection has three features that make it particularly suitable to address the systemic challenges of the digital society and further the objectives of digital constitutionalism. These are its protective nature, its dialogic procedural structure and its universality. Data protection, like all other fundamental rights, should not simply be dismissed due to selected

failures or inefficiencies. There is a value in fundamental rights that cannot be easily replicated by other legal instruments.