The rise of digital constitutionalism in the European Union

Giovanni De Gregorio*

In the last twenty years, the policy of the European Union in the field of digital technologies has shifted from a liberal economic perspective to a constitution-oriented approach. This change of heart has resulted primarily from the rise of the information society which has created not only new opportunities but also challenges to fundamental rights and democratic values. Even more importantly, this technological framework driven by liberal ideas has empowered transnational corporations operating in the digital environment to perform quasi-public functions on a global scale. This article analyzes the path and the reasons that have led the European Union to enter a new phase of modern constitutionalism (i.e. digital constitutionalism). The primary goal of this article is to describe the characteristics of this new constitutional phase opposing platform powers, and to outline the potential evolution of European digital constitutionalism in the global context.

1. Introduction

In the last twenty years, the policy of the European Union (EU) in the field of digital technologies has shifted from a liberal economic perspective to a constitutional approach aimed to protect fundamental rights and democratic values. In order to understand this change of heart, it is necessary to frame the debate in the information society which is increasingly subject to the power of public and private actors implementing automated decision-making technologies.[1] If the digital environment, as a new space where information and data flow, has been an opportunity to offer cross-border services and exercise individual freedoms, it has also led to serious challenges for constitutional law. Since the end of the last century, the development of digital technologies has not only challenged the protection of individuals' fundamental rights, such as freedom of expression, privacy, and data protection. Even more importantly, this technological

* PhD Candidate, University of Milano-Bicocca, Milan, Italy; Academic Fellow, Bocconi University, Bocconi, Italy. Email: degregorio.giovanni@unibocconi.it.

[1] John Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation*, 29(3) Phil. & Tech. 245 (2016).

framework driven by liberal ideas has also empowered transnational corporations operating in the digital environment, primarily online platforms, to perform quasi-public functions in the transnational context, thus competing with public actors.

Therefore, the debate is no longer locked into the field of private or competition law but is shifting to a public law perspective, and precisely a digital constitutional angle.[2] Among its roles, modern constitutionalism aims to protect fundamental rights and limit the emergence of powers outside any control.[3] Constitutions have been developed in view of limiting governmental powers and, thus, shielding individuals from interference by public authorities. From a constitutional law perspective, the notion of power has traditionally been vested in public authorities; a new form of (digital) private power has now arisen due to the massive capability of organizing content and processing data. Therefore, the primary challenge involves not only the role of public actors in regulating the digital environment, but also, more importantly, the "talent of constitutional law" to react against the threats to fundamental rights and the rise of private powers, whose nature is much more global than local.

These drivers have pushed the Union to enter a new phase of European constitutionalism (i.e. digital constitutionalism). A new phase in European (digital) constitutionalism is rising as a shield against the discretionary exercise of power by online platforms in the digital environment. As Suzor observes, "digital constitutionalism requires us to develop new ways of limiting abuses of power in a complex system that includes many different governments, businesses, and civil society organizations."[4] Put differently, digital constitutionalism consists of articulating the limits to the exercise of power in a networked society.[5]

Within this framework, this article analyzes the path and the reasons that have led the EU policy to move from a liberal to a constitutional approach to the digital environment in the last thirty years. The primary goal is to describe the characteristics of digital constitutionalism as a new constitutional phase. This article aims to explain this paradigmatic shift by focusing on threats to fundamental rights and the rise of private

[2] Recently, scholars have approached the power of online platforms from different perspectives. *See* Julie Cohen, Between Truth and Power. The Legal Construction of Informational Capitalism (2020); Nicolas Petit, Big Tech and the Digital Economy (2020); Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the State*, 72 SMU L. Rev. 27 (2019); Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2018); Natali Helberger et al., *Governing Online Platforms: From Contested to Cooperative Responsibility*, 34 Info. Soc'y 1 (2018); Niva Elkin-Koren & Maayan Perel, *Algorithmic Governance by Online Intermediaries*, *in* The Oxford Handbook of Institutions of International Economic Governance and Market Regulation (Eric Brousseau et al. eds., 2018); Digital Dominance: The Power of Google, Amazon, Facebook, and Apple (Martin Moore & Damian Tambini eds., 2018); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv. L. Rev. 1598 (2018); How Platforms are Regulated and How They Regulate Us (Luca Belli & Nicolo Zingales eds., 2017).

[3] Jeremy Waldron, *Constitutionalism: A Skeptical View* (N.Y.U. School of Law, Public Law Research Paper No. 10–87, May 1, 2012), https://ssrn.com/abstract=1722771; European Constitutionalism Beyond the State (Joseph H. H. Weiler & Marlene Wind eds., 2003).

[4] Nicolas Suzor, Lawless: The Secret Rules That Govern Our Digital Lives 173 (2019).

[5] Claudia Padovani & Mauro Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System*, 80 Int'l Comm. Gazette 295 (2018).

powers in the algorithmic society. Furthermore, this study outlines the potential evolution of European digital constitutionalism, underlining the role of the European policy in the global context.

This article aims to provide a new contribution to enrich the status quo of the scholarly debate from at least two standpoints. First, it describes the challenges to constitutionalism in the algorithmic society from a European constitutional law perspective, focusing on the fields of content and data.[6] Second, while other works have primarily focused on digital constitutionalism as a new constitutional moment[7] or mapping bill of rights and legislative attempts concerning the relationship between Internet and constitutions,[8] this article examines the rise and consolidation of a new phase of European (digital) constitutionalism as an example of how constitutional law can react against the challenges of the algorithmic society, with specific regard to the role of online platforms. Although the challenges coming from the implementation of these technologies also involve public actors, this work argues that the reaction of European constitutionalism primarily comes from the threats to fundamental rights and democratic values raised by new private powers in the algorithmic society.

In order to achieve these goals, this article defines three phases across which the EU has moved from a digital liberal approach to a constitutional-oriented strategy, precisely digital liberalism, judicial activism and digital constitutionalism. The analysis of each phase focuses on the fields of content and data as examples of the evolution of the EU policy, as also influenced by the role of the Council of Europe. Section 2 focuses on framing the first regulatory steps taken by the Union in the field of content and data at the end of the last century. Section 3 analyzes the role and efforts of the Court of Justice of the European Union (CJEU) in underlining the relevance of fundamental rights online in the aftermath of the adoption of the Lisbon Treaty. Section 4 focuses on the rise of digital constitutionalism in the framework of the European Digital Single Market (DSM) strategy. Section 5 describes the primary findings of this work and underlines the potential evolution of European digital constitutionalism in the global context.

2. The first phase: Digital liberalism

Following the signing of the Treaty of Rome in 1957, the primary goal of the European Economic Community was the establishment of a common market and the approximation of economic policies among member states.[9] These economic roots could be considered the original imprinting of the Union in the field of digital technologies.

[6] For an Australian perspective, see Monique Mann, *The Limits of (Digital) Constitutionalism: Exploring the Privacy–Security (Im)balance in Australia*, 80 Int'l Comm. Gazette 369 (2018).

[7] Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorization*, 33(1) Int'l Rev. L., Computers & Tech. 76 (2019).

[8] Dennis Redeker et al., *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 80 Int'l Comm. Gazette 302 (2018); Mauro Santaniello et al., *The Language of Digital Constitutionalism and the Role of National Parliaments*, 80 Int'l Comm. Gazette 320 (2018).

[9] Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 3, 4 Eur. Y.B. 412 [hereinafter Treaty of Rome]. *See also* Kamiel Mortelmans, *The Common Market, the Internal Market and the Single Market: What's in a Market?*, 35(1) Common Mkt. L. Rev. 101 (1998).

Until the adoption of the Nice Charter in 2000 (EU Charter) and the recognition of its binding effects in 2009,[10] the EU approach was firmly based on its economic pillars, namely the fundamental freedoms.[11] The regulation of the digital environment is a paradigmatic example of the transposition of this liberal approach into EU law and, therefore, member states' legal systems. It would be sufficient to take as examples Directive 95/46/EC (Data Protection Directive) and Directive 2000/31/EC (e-Commerce Directive) to understand how the policy goal of the Union oriented to liberal values to ensure the smooth development of the internal market.[12]

Such a liberal approach in the field of content and data should not surprise if it is framed within the debate about Internet regulation at the end of the twentieth century, when the online environment was considered an area outside public actors' interference. In the "Declaration of Independence of Cyberspace,"[13] Barlow maintains that the digital space is a new world separate from the atomic one, where "legal concepts of property, expression, identity, movement, and context do not apply."[14] This world independent from physical location was also supported by Johnson and Post,[15] who consider a decentralized and emergent law, resulting from customary or collective private action, the basis for creating a democratic set of rules applicable to the digital community.[16] In other words, these ideas are based on a bottom-up approach: rather than relying on traditional public lawmaking power to set the rules of cyberspace, every digital community would be capable of participating in the creation of the new rules governing their digital world.[17] Therefore, self-regulation would provide a better regulatory framework than centralised rulemaking.[18]

[10] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391 [hereinafter EU Charter].

[11] Consolidated version of the Treaty on the Functioning of the European Union, titles II and IV, 2012 O.J. (C 326) 47 [hereinafter TFEU].

[12] 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 O.J. (L 281) 31 [hereinafter Data Protection Directive]; 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, 2000 O.J. (L 178) 1 [hereinafter e-Commerce Directive].

[13] John P. Barlow, *A Declaration of Independence of the Cyberspace*, Electronic Frontier Found. (Feb. 8, 1996), www.eff.org/cyberspace-independence.

[14] *Id.*

[15] David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1371 (1996).

[16] David R. Johnson & David Post, *And How Shall the Net Be Governed?*, *in* Coordinating the Internet 62 (Brian Kahin & James Keller eds., 1997).

[17] Scholars criticized these positions, underlining the possibility for states to regulate the digital environment. *See* Lawrence Lessig, Code 2.0: Code and Other Laws of Cyberspace (2006); Joseph H. Sommer, *Against Cyberlaw*, 15 Berkeley Tech. L.J. 1145 (2000); Jack L. Goldsmith, *Against Cyberanarchy*, 40 U. Chi. L. Occasional Paper 1 (1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553 (1997–1998).

[18] I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. Pitt. L. Rev. 993 (1994).

These libertarian theories are based on a single fundamental assumption. The characteristics of the digital environment would oblige governments and lawmakers to adopt a free market-based regulation. In one of his works, Froomkin defines the Internet as the "Modern Hydra."[19] Every time someone cuts the heads of the mythical beast off, new ones grow. The same parallelism occurs when regulators attempt to interfere with the online environment (cutting off one of Hydra's heads) and users easily circumvent the new rules (the growth of new heads).

This metaphor illustrates not only the tradeoff that governments faced at the end of the last century between innovation and protection of constitutional rights, but also why (democratic) states have adopted a free market approach in relation to the digital environment (i.e. digital liberalism).[20] Since the adoption of a paternalistic approach could hinder the development of new digital services, it should not surprise if the EU was more concerned about the potential impacts of regulatory burdens on economic freedoms and innovation than about the protection of individuals' rights and freedoms. At the time, there were no reasons to fear the rise of new private powers challenging the protection of fundamental rights while competing with state power. An extensive regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were poised to revolutionize the entire society. In other words, with the advent of the Internet, the European approach was comprehensively far from digital constitutionalism, because digital technologies were considered more as an opportunity to grow and prosper rather than a way to exercise powers.

Within this framework, this section analyzes how this liberal framework has characterized the EU policy at the beginning of this century. By looking at the first regulatory steps in the field of data and content, the next subsections focus on the e-Commerce Directive and Data Protection Directive.

2.1. Content: The e-Commerce Directive

The adoption of the e-Commerce Directive can be considered a paradigmatic example of the European liberal approach. As the analysis of the first Recitals can reveal, the primary aim of the e-Commerce Directive is to provide a common framework for electronic commerce for "the proper functioning of the internal market by ensuring the free movement of information society services between the Member States." [21]

When the US Congress passed section 230 of the Communication Decency Act in 1996,[22] the primary aim was to encourage free expression and development of the digital environment.[23] In order to achieve this objective, the choice was to exempt

[19] A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* Borders in Cyberspace 129 (Brian Kahin & Charles Nesson eds., 1997).

[20] Governments have not adopted the same free-market approach concerning the Internet as China and the Arab states did. *See* Barney Warf, *Geographies of Global Internet Censorship*, 76 GeoJ. 1 (2011); Anupam Chander & Uyen P. Le, *Data Nationalism*, 64(3) Emory L.J. 677 (2015).

[21] e-Commerce Directive, *supra* note 12, recitals 1–3.

[22] Communication Decency Act, 47 U.S.C. § 230.

[23] Jeff Kosseff, The Twenty-Six Words That Created the Internet (2016).

computer services from liability for hosting third-party content. Before the adoption of section 230, some cases had already made clear how online intermediaries would have been subject to a broad and unpredictable range of cases concerning their liability for editing third-party content.[24] Since this risk would have slowed down the development of new digital services in the aftermath of the Internet, online intermediaries have been encouraged to grow and develop their business under the protection of the Good Samaritan rule.[25]

Within this framework, the e-Commerce Directive establishes a regime of exemption of liability for Internet service providers (or "online intermediaries").[26] Based on the US "safe harbor" model introduced at the end of the last century by the Communication Decency Act and the Digital Millennium Copyright Act,[27] this regime acknowledges the passive role of online intermediaries lacking any involvement in the creation of content, and exempts them from liability for transmitting or hosting unlawful third-party content.[28]

Likewise, the aim of the EU liability exemption is twofold. First, the e-Commerce Directive aims to foster the development of the internal market through the free movement of information society services as a "reflection in Community law of a more general principle, namely freedom of expression,"[29] enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[30] Second, this special regime does not hold liable entities that do not have effective control over third-party content. In order to achieve these purposes, the e-Commerce Directive sets forth a general rule consisting of a ban on general monitoring.[31] Therefore, member states cannot oblige online intermediaries to monitor the information transmitted or stored by users within their services, and online intermediaries are not required to seek facts or circumstances that reveal illegal activities conducted by their users through the relevant service.[32] Furthermore, among online intermediaries,[33] hosting providers are not liable for the information or content stored by their users unless, upon becoming aware of the unlawful nature of the

[24] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Services Co., WL 323710 (N.Y. Sup. Ct. 1995).

[25] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[26] Edward Halpin & Seamus Simpson, *Between Self-Regulation and Intervention in the Networked Economy: The European Union and Internet Policy*, 28(4) J. Info. Sci. 285 (2002).

[27] Digital Millennium Copyright Act, 17 U.S.C. § 512.

[28] The Responsibilities of Online Service Providers (Mariarosaria Taddeo & Luciano Floridi eds., 2017); Secondary Liability of Internet Service Providers (Graeme Dinwoodie ed., 2017).

[29] e-Commerce Directive, *supra* note 12, recital 9.

[30] European Convention on Human Rights, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

[31] *Id.*, art. 15.

[32] Nevertheless, when implementing the e-Commerce Directive in their respective national legislation, member states are free to impose on Internet service providers a duty to report to the competent public authority possible illegal activity conducted through their services or the transmission or storage within their services of unlawful information. *Id.* art. 15(2).

[33] This ban applies to three categories of online intermediaries: access providers, caching providers, and hosting providers: *see* e-Commerce Directive, *supra* note 12, arts. 12–14.

information or content stored, they do not promptly remove or disable access to the unlawful information or content.[34]

This legal framework shows how online intermediaries have been generally considered neither accountable nor responsible for transmitted or hosted content (i.e. safe harbor) since platforms are not aware (or in control) of illicit content in their digital rooms. Although this consideration could be accepted, provided that online intermediaries performed only passive activities, such as providing access or digital space to host third-party content, the same approach has been challenged with the evolving framework of e-commerce platforms and social media profiting from the organization and moderation of content through artificial intelligence technologies.

Therefore, if, on the one hand, this political choice was aimed at ensuring the development of the internal market in the aftermath of the Internet, on the other hand, such a liberal approach has contributed to the rise and consolidation of online platforms in the internal market. By imposing upon hosting providers an obligation to remove online content based on their awareness (i.e. "notice and takedown"), this system of liability has entrusted online intermediaries with the power to autonomously decide whether to remove or block vast amounts of content based only on the risk of being held liable. Since online platforms are privately run, these actors would attempt to avoid the risk of being sanctioned for non-compliance with this duty by removing or blocking even that content whose illicit nature is not fully evident (i.e. collateral censorship).[35] This liability regime incentivizes online platforms to focus on minimizing this economic risk rather than adopting a fundamental rights-based approach. As a result, this system of liability works as a legal shield for online intermediaries,[36] and, even more importantly, it encourages online platforms to set their rules to organize and moderate content based on the risk of being sanctioned and opaque business logic.[37]

This incentive (or indirect delegation) to moderate content can be considered one of the primary reasons explaining how online platforms have acquired broad margins in determining the scope of protection of fundamental rights in the digital environment. As this article explains, the turning of economic freedom into a new form of power is one of the primary challenges which led to the rise of European digital constitutionalism.

2.2. Data: The Data Protection Directive

In the field of data, the European liberal approach is counterintuitive. At first glance, the EU has not followed a liberal regulatory path. Rather than exempting online

[34] *Id.* art. 14.

[35] Regarding the risk of collateral censorship, see Delfi AS v. Estonia, June 15, 2016, https://bit.ly/2LglTMF; MTE v. Hungary, Feb. 2, 2016, https://bit.ly/38X2fxF. *See* Jack Balkin, *Old-School/New-School Speech Regulation*, 128 Harv. L. Rev. 2296 (2014); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87(1) Notre Dame L. Rev. 293 (2011).

[36] Frank Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, 17 Theoretical Inquiries in L. 487 (2016); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986 (2008).

[37] Klonick, *supra* note 2; Danielle K. Citron & Helen L. Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age*, 91 B. U. L. Rev. 1436 (2011).

intermediaries from liability even in the field of data, the EU decided to regulate the processing of personal data to face the challenges coming from the increase in data usage and processing relating to the provision of new services and the development of digital technologies.[38]

The rise and consolidation of data protection law can be explained as a response to the information society driven by new technologies and, primarily, automated systems implemented by public and private entities to process data. In other words, if the right to privacy were enough to meet the interests of individuals' protection,[39] in the information society the massive processing of personal data has made it no longer sufficient to protect only the negative dimension of the right to privacy, thus leading to the rise of a positive dimension fostering the degree of transparency and accountability in data processing.[40]

Whilst the Council of Europe played a crucial role in consolidating the constitutional dimension of the right to privacy and data protection in Europe,[41] this consideration can be only partially extended to the EU since data protection has been recognized as a fundamental right by the Nice Charter only five years after the adoption of the Data Protection Directive. In 1995, the EU policy was oriented to an economic approach toward the free movement of data. The Data Protection Directive highlights the functional nature of the protection of personal data for the consolidation and proper functioning of the internal market and, consequently, as an instrument to guarantee European fundamental freedoms.[42] Although the Data Protection Directive highlighted that the processing of personal data shall serve mankind and aim to protect the fundamental right to privacy of data subjects,[43] the economic-centric frame with regard to the protection of personal data cannot be disregarded. The liberal imprinting of the Data Protection Directive can be understood by focusing on the first proposal of the Commission in 1990.[44]

From an *ex-post* perspective, both the time of adoption and the lack of any review in more than twenty years could explain why European data protection law had shown its fallacies before the challenges were raised by online platforms in the digital environment. At the end of the last century, the EU could not foresee how the digital environment would affect the right to privacy and data protection. At that time, the actors operating in the digital environment were online intermediaries offering the storage, access, and transmission

[38] Data Protection Directive, *supra* note 12, recital 4.

[39] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[40] Serge Gutwirth & Paul De Hert, *Regulating Profiling in a Democratic Constitutional States*, *in* Profiling the European Citizen 271, 271 (Mireille Hildebrandt & Serge Gutwirth eds., 2006).

[41] *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS 108. This international legal instrument has been amended in 2018. *See* Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15.final (May 18, 2018). *See, e.g.*, Leander v. Svezia, 9 E.H.R.R. 433 (1987); Amann v. Switzerland, 30 E.H.R.R. 843 (2000); S. and Marper v. The United Kingdom, 48 E.H.R.R. 50 (2008).

[42] Data Protection Directive, *supra* note 12, recital 3.

[43] *Id.* recital 2.

[44] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final (Sept. 13, 1990).

of data across networks. There were no social media platforms, e-commerce marketplaces, or other digital services: the role of intermediaries was merely passive. However, post 1995, the first draft of reviewing the privacy and data protection regime was proposed only in 2012,[45] and the General Data Protection Regulation (GDPR) entered into force in 2016, even without any binding effect until May 2018.[46] In other words, the (digital) liberal approach of the EU in this field has resulted from an omissive approach.

Moreover, the characteristics of EU directives can explain another reason for the inadequacy of the European data protection law to face transnational digital challenges. Unlike regulations which are applicable in member states' internal law immediately after its entry into force, directives provide just the result to be achieved and are not generally applicable without domestic implementation.[47] Therefore, the margin of discretion in implementing the Data Protection Directive at member states' level is another reason for the legal fragmentation in the field of data protection. Even if these considerations could also be extended to the e-Commerce Directive, however, in this case, the heterogeneous legal system of data protection in Europe coming from the mix of different domestic traditions and margin of discretions left by the Data Protection Directive to the member states can be considered one of the primary obstacles for data protection law to face uniformly the challenges of the information society.

Within this framework, the fragmentation of domestic regimes and the lack of any revision have been the primary drivers encouraging the evolution of forms of freedoms into power based on the processing of vast amounts of (personal) data on a global scale. In other words, in the field of data, the rise and consolidation of new actors in the digital environment have been the result not only of the liberal frame but also of the regulatory design and omissive approach of the EU since the adoption of the Data Protection Directive. Like in the field of content, the shift from freedom to power shows why the EU has approached a new (digital) constitutional strategy.

3. The second phase: Judicial activism

The end of the first (liberal) phase is the result of two events which have, at the very least, triggered a new phase of judicial activism. The first event concerned the

[45] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final (Jan. 25, 2012).

[46] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. This approach is also shown by the lack of review of the e-privacy framework as governed by Directive 2002/58/EC. *See* Directive 2002/58/EC (Directive on privacy and electronic communications) 2002 O.J. (L 201); Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final (Jan. 10, 2017).

[47] TFEU, *supra* note 11, art. 288.

emergence of new actors in the digital environment (i.e. online platforms), whereas the second involved the increasing role of the EU Charter as a bill of rights of the European Union.[48]

The first transformation concerns the role of online intermediaries, precisely hosting providers. At the end of the last century, these entities provide access to, host, transmit, and index content, products, and services originated by third parties on the Internet or provide Internet-based services to third parties. In other words, online intermediaries were mere service providers without being involved in the moderation of content or the processing of personal data.

These considerations cannot be applied to the role that some hosting providers, such as social media platforms and search engines, have been playing since approximately the first decade of this century. This difference can be explained by looking at the platforms' business models which are primarily data driven.[49] In the case of social media, the primary activities of these actors do not consist of providing free online spaces where users can share information and opinions. On the contrary, social media gain profits from advertising based on profiling users' data.[50] Here, the intimate relationship between content and data is unveiled. In order to ensure a safe digital environment for users and avoid their escape, platforms rely on automated decision technologies to moderate online content and capture users' attention.[51] The increasing involvement of platforms in the organization of content and the profiling of users' preferences using artificial intelligence technologies has transformed the role of online platforms as hosting providers. In other words, while the exemption of liability for online intermediaries and the data protection regime were introduced when these actors played only passive roles, today the use of automated systems to filter and process preferences has led these entities to perform organizational activities whose passive nature makes them more difficult to support.

Second, the recognition of the binding nature of the EU Charter and its inclusion in EU primary law have contributed to codifying the constitutional dimension of the European (digital) environment.[52] Until that moment, the protection of freedom of expression, privacy, and data protection in the European context was based not only on the domestic level but also on the ECHR.[53] The Strasbourg Court has played a crucial role not only in protecting the fundamental rights but also in underlining the constitutional challenges coming from digital technologies.[54]

48 Grainne De Burca, *After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, 20 Maastricht J. Eur. & Comp. L. 168 (2013).

49 Nick Srnicek, Platform Capitalism (2016).

50 Asunción Esteve, *The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA*, 7 Int'l Data Privacy L. 36 (2017).

51 Tarleton Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (2018); Tim Wu, The Attention Merchants: The Epic Scramble to Get Inside our Heads (2016).

52 Consolidated version of Treaty on the European Union, art. 6(1), 2012 O.J. (C 326)13.

53 ECHR, *supra* note 30, arts. 8, 10.

54 Oreste Pollicino, *Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech*, 25 Eur. L.J. 155 (2019).

The adoption of the Lisbon Treaty has constituted the further step in this process. The right to freedom of expression,[55] private and family life,[56] and the protection of personal data,[57] as already enshrined in the Nice Charter, have become binding vis-à-vis member states and EU institutions,[58] which can interfere with these rights only according to a test established by Article 52 of the EU Charter.[59] Besides, the EU Charter adds another important piece in the European constitutional puzzle by prohibiting the abuse of rights consisting of the "destruction of any of the rights and freedoms recognized in this Charter or at their limitation to a greater extent than is provided for herein."[60]

Within this new constitutional framework, the CJEU started to rely on the EU Charter to answer the challenges raised by the digital environment. Both in the field of content and data, the CJEU interpreted the EU Charter's rights and freedoms with the aim to ensure the effective protection of these constitutional interests. As the next subsections show, given the lack of any legislative review of either the e-Commerce Directive or the Data Protection Directive, judicial activism has highlighted the challenges to fundamental rights in the information society, thus promoting the transition from a mere economic perspective to a new constitutional phase of European (digital) constitutionalism.

3.1. Content: From economic interests to fundamental rights

The steps forward taken by the CJEU in the aftermath of the Lisbon Treaty unveiled the constitutional dimension of online platforms' liability system. However, before 2009, the CJEU's case law focused on the boundaries of this liability regime in two landmark decisions just from an economic perspective.

In *Google France*,[61] the CJEU concluded that, where an Internet-referencing service provider had not played an active role so as to obtain knowledge of, or control over, the data stored, it could not be held liable for the data that it had stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of that data or of that advertiser's activities, it had failed to act expeditiously to remove, or to disable access to, the data concerned. The liberal frame of this decision can be understood by looking at the opinion of the Advocate General in this case. According to Poiares Maduro, search engine results are a "product of automatic algorithms that apply objective criteria in order to generate sites likely to be of interest to the internet user," and, therefore, even if Google has a pecuniary interest in providing users with the

[55] EU Charter, *supra* note 10, art. 11(1).

[56] *Id.* art. 7.

[57] *Id.* art. 8(1).

[58] *Id.* art. 51.

[59] Koen Lenaerts, *Exploring the Limits of the EU Charter of Fundamental Rights*, 8 Eur. Const. L. Rev. 375 (2013).

[60] EU Charter, *supra* note 10, art. 54.

[61] Cases C-236/08, C-237/08, and C-238/08, Google France v. Louis Vuitton Malletier SA, Google France SARL v. Viaticum SA and Luteciel SARL, and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and others, 2010 E.C.R. I-02417 (Mar. 23, 2010).

possibility to access the more relevant sites, "it does not have an interest in bringing any specific site to the internet user's attention."[62] Although the Advocate General did not recognize the active role of this provider, the liberal frame of this opinion and the role of automated processing systems had already shown their relevance in the field of online content.

A step forward was made in *L'Oréal*.[63] The Court recognized that offering assistance, including the optimization, presentation, or promotion of sale offers, was not a neutral activity performed by the provider in question according to recital 42.[64] Although the Court has not expressly recalled the opinion of Poiares Maduro in *Google France*, this decision acknowledged, first of all, how automated technologies have led some providers to perform an active role, rather than the mere passive provision of digital products and services.

In 2011, the CJEU shifted its approach from a merely economic perspective to a fundamental rights-based approach. It is not by accident that this turning point occurred in the wake of the Lisbon Treaty recognizing that the EU Charter has the same legal value as EU primary law. The Court, first, addressed two cases involving a ban on general monitoring applying to online intermediaries. In *Scarlet* and *Netlog*,[65] the question concerned prohibiting member states from imposing a general obligation on providers to monitor the information that they transmit or store. The primary question concerned the proportionality of such an injunction. In these cases, according to the CJEU, an injunction to install a general filtering system would not respect online intermediaries' freedom to conduct business.[66] Moreover, the contested measures could affect users' fundamental rights, namely their right to the protection of their personal data and their freedom to receive or impart information.[67] The CJEU dealt with the complex topic of finding the balance between the fundamental rights of the users, especially the right to data protection and freedom of expression, and the interests of the platforms not to be overwhelmed by expensive monitoring systems. The Court held that Belgian content filtering requirements "for all electronic communications [. . .]; which applies indiscriminately to all its customers; as a preventive

[62] Cases C-236/08, C-237/08, and C-238/08, Google France v. Louis Vuitton Malletier SA, Google France SARL v. Viaticum SA and Luteciel SARL, and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and others, Opinion of Advocate General Poiares Maduro (Sept. 22, 2009), at 144.

[63] Case 324/09, L'Oréal SA and Others v. eBay International AG and Others, 2011 E.C.R. I-06011 (July 12, 2011). *See* Patrick Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, 48 Common Mkt. L. Rev. 1455 (2011).

[64] Case 324/09, L'Oreal, 2011 E.C.R. I-06011, at 124.

[65] *See* Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 (Nov. 24, 2011) [hereinafter Scarlet]; Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, ECLI:EU:C:2012:85 (Feb. 16, 2012) [hereinafter SABAM]. *See* Stefan Kulk & Frederik Zuiderveen Borgesius, *Filtering for Copyright Enforcement in Europe after the* Sabam *Cases*, 34(11) EIPR 791 (2012).

[66] C-70/10, Scarlet, 2011 E.C.R. I-11959, at 50.

[67] EU Charter, *supra* note 10, arts. 8, 11.

measure; exclusively at its expense; and for an unlimited period" violated the ban on general monitoring obligation.

Since that time, the CJEU has relied on the Charter to adjudicate other cases involving online intermediaries. For example, in *Telekabel* and *McFadden*,[68] the CJEU referred to two other cases involving injunction orders on online intermediaries which leave the provider free to choose the measures to tackle copyright infringement, while maintaining the exemption of liability, thus showing its duty of care in respect of EU fundamental rights. The CJEU upheld the interpretation of the referring national court on the same (constitutional) basis argued in *Scarlet* and *Netlog*, by concluding that the fundamental rights recognized by EU law must be interpreted as not precluding a court injunction such as that of the case in question.

Despite these judicial efforts, the CJEU did not solve the issues raised by online platforms. The liability for actively organizing third-party content, as well as the lack of transparency and accountability in content moderation, are still two primary challenges in the field of content. As the next section shows, the implementation of automated decision-making technologies to moderate content questions not only the system of the e-Commerce Directive but also democratic values, such as the protection of fundamental rights and the rule of law. Within this framework, the rise of European digital constitutionalism is a reaction against the power exercised by online platforms, which are increasingly involved in determining the scope of rights and freedoms in the information society. Nonetheless, the EU is not just reacting to, but also setting a strategy toward, transparency and accountability in content moderation.

3.2. Data: The judicial path towards digital privacy

The CJEU has not only contributed to fostering the protection of fundamental right in relation to online content, but also to consolidating and emancipating the right to data protection in the European framework.[69] As in the case of online content, the recognition of the EU Charter as a primary source of EU law and the increasing relevance of data in the information society have encouraged the CJEU to complement the economic-functional dimension of the Data Protection Directive with a constitutional approach, as demonstrated by the decisions on digital privacy in the wake of the Lisbon Treaty. As a first step, in the *Promusicae* case,[70] the Court has recognized the relevance of data protection, "namely the right that guarantees protection of personal

[68] *See* Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, ECLI:EU:C:2014:192 (Mar. 27, 2014); Case C-484/14, Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, ECLI:EU:C:2016:689 (Sept. 15, 2016). *See also* Martin Husovec, *Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours*, 12 J. Intell. Prop. L. & Prac. 115 (2017).

[69] *See* Orla Lynskey, The Foundations of EU Data Protection Law (2015); Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, *in* Reinventing Data Protection 3 (Serge Gutwirth et al. eds., 2009).

[70] Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-271, at 63 (Jan. 29, 2008).

data and hence of private life,"[71] despite the functional link with the protection of privacy.[72]

Some years later, in *Digital Rights Ireland*,[73] the Court invalidated Directive 2006/24/EC due to its disproportionate effects on fundamental rights,[74] by assessing, as a constitutional court, the interference with and potential justifications of the rights of privacy and data protection of EU citizens established by the EU Charter.[75] The CJEU has shown itself to be aware of the risks of new technologies to the protection of the fundamental rights of EU citizens. Indeed, the retention of all traffic data "applies to all means of electronic communication. [. . .] It therefore entails an interference with the fundamental rights of practically the entire European population."[76] Moreover, concerning automated technologies, the CJEU observed that "[t]he need for such safeguards is all the greater where [. . .] personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data."[77]

The same constitutional approach can be appreciated in *Schrems*,[78] where the CJEU invalidated Decision 2000/520,[79] which was the legal basis allowing the transfer of data from the EU to the United States (i.e. safe harbor).[80] In this case, the interpretation of the CJEU can be considered an extensive interpretation of the regime of data transfer which required "an adequate level of protection by reason of its domestic law or its international commitments" with the aim of ensuring "the protection of the private lives and basic freedoms and rights of individuals."[81] The CJEU manipulated the notion of "adequacy," which, as a result of this new constitutional frame, has

[71] *Id.* at 63.

[72] Juliane Kokott & Christoph Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 Int'l Data Privacy L. 222 (2013).

[73] Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238 (Apr. 8, 2014) [hereinafter *Digital Rights Ireland*]. *See, in particular*, Federico Fabbrini, *The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the U.S.*, 28 Harv. Hum. Rts. J. 65 (2015).

[74] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105), at 54.

[75] *See, more recently*, Case C-511/18, La Quadrature du Net and Others v. Premier ministre and Others, ECLI:EU:C:2020:791 (Oct. 6, 2020).

[76] Cases C-293/12 & C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, at 56.

[77] *Id.* at 55.

[78] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015). *See, in particular*, Oreste Pollicino & Marco Bassini, *Bridge Is Down, Data Truck Can't Get Through . . .: A Critical View of the* Schrems *Judgment in the Context of European Constitutionalism*, 16 Global Community Y.B. Int'l L. & Juris. 245 (2017).

[79] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7.

[80] *See, more recently*, Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

[81] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), at 71.

moved to a standard of "equivalence" between legal orders.[82] Therefore, according to the CJEU, the adequate level of protection required of third states for the transfer of personal data from the EU should ensure a degree of protection essentially equivalent to the EU's "by virtue of Directive 95/46 read in the light of the Charter."[83]

The two above-mentioned cases underline the role of the Charter in empowering and extending (or adapting) the scope of the Data Protection Directive vis-à-vis the new digital threats coming from massive processing of personal data both inside and outside the EU boundaries. Nevertheless, the case showing the paradigmatic shift from an economic to a constitutional perspective in the field of data is *Google Spain*, for at least two reasons.[84]

First, as in *Digital Rights Ireland* and *Schrems*, the Court granted a high level of protection to privacy and data to ensure the effective protection of these fundamental rights by virtue of a (constitutional) interpretation. Second, the *Google Spain* case demonstrates a first judicial attempt to face the power of online platforms and address the legislative inertia of the EU, thereby laying a foundation for European digital constitutionalism.

The predominant role of Articles 7 and 8 can be observed by focusing on how the CJEU recognized that a search engine like Google falls under the category of "data controller." Indeed, when interpreting the scope of application of the Data Protection Directive, the CJEU observed that:

> [I]t would be contrary not only to the clear wording of that provision but also to its objective—which is to ensure [. . .] effective and complete protection of data subjects—to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.[85]

Second, the same consideration also applies to the definition of establishment. The CJEU ruled that that processing of personal data should be considered as being conducted in the context of the activities of an establishment of the controller in the territory of a member state, within the meaning of that provision, when the operator of a search engine sets up, in a member state, a branch or subsidiary that is intended to promote and sell advertising space offered by that engine and that orientates.

> Its activities toward the inhabitants of that member state.[86] As the CJEU observed, it cannot be accepted that the processing of personal data [. . .] should escape the obligations and guarantees laid down by Directive 95/46, which would compromise [. . .] the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to.[87]

[82] *Id.* at 73.

[83] *Id.*

[84] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317 (May 13, 2014) [hereinafter Google Spain]; Orla Lynskey, *Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez*, 78 Mod. L. Rev. 522 (2015).

[85] Case C-131/12, Google Spain, ECLI:EU:C:2014:317, at 34.

[86] *Id.* at 58.

[87] *Id.* at 60.

Third, the CJEU has entrusted search engines with delisting online content without removing information. Hence, the data subject has the right to request that the search engine obtain the erasure of a link to the information relating to him or her from a list of web results based on his or her name, "in the light of his fundamental rights under Articles 7 and 8 of the Charter."[88] As a result, one can argue that this interpretation has unveiled a legal basis for data subjects to enforce their rights against private actors. The CJEU has recognized a right to be forgotten online through its interpretation of the Data Protection Directive or the horizontal application (*de facto*) of Articles 7 and 8 of the Charter. Despite this high level of protection of fundamental rights and the limitations on private actors' activities, at the same time, the CJEU has delegated to search engines the task of balancing fundamental rights when assessing users' requests for the right to be forgotten.[89]

As underlined in the case of online content, judicial activism has not been enough to solve the issue raised in the field of data, thus requiring a step forward. Although the role of the CJEU has been important to consolidate the constitutional dimension of privacy and data protection in the Union, the next section shows how the GDPR has tried to address the fallacies of EU data protection law, being one of the primary expressions of European digital constitutionalism.

4. The third phase: Digital constitutionalism

Technological evolution, combined with a liberal constitutional approach, has led online platforms to acquire a predominant role in the digital environment. The massive reliance on algorithmic technologies to moderate content and process data has not only led to new ways and models to extract value from information.[90] These technologies have also contributed to making platform decision-making more opaque, thus, raising questions about transparency and accountability.[91] Besides, these technologies have raised concerns for the protection of fundamental rights,[92] such as freedom of expression and privacy, as well as democratic values in the information society.[93]

[88] *Id.* at 97.

[89] Jean-Marie Chenou & Roxana Radu, *The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union*, 58 Bus. & Soc'y 74 (2017).

[90] Luciano Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality (2014).

[91] Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, 3 Big Data & Soc'y (2016), https://bit.ly/3nlpYNX; Brent D. Mittlestadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 Big Data & Soc'y (2016), https://bit.ly/3pbkru3.

[92] Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. Davis L. Rev. 1151 (2018).

[93] Paul Nemitz, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, 2133 Philos. Trans. Royal Soc. A 89 (2018).

Digital firms are no longer market participants, since they "aspire to displace more government roles over time, replacing the logic of territorial sovereignty with functional sovereignty."[94] It is not by accident that these actors have been named "gatekeepers" to underline their high degree of control on online spaces.[95] Users are subject to the exercise of a "private" form of authority exercised by online platforms through a mix of private law and automated technologies (i.e. the law of the platforms). By privately regulating their digital infrastructure, online platforms can autonomously decide not only how people interact, but also how they can assert their rights.[96] In the absence of any regulation, these business choices fulfill the role of the law in the digital environment on a global scale. Precisely by implementing terms of service (ToS), platforms unilaterally establish the rules with which users have to comply when accessing providers' services, and which determine how their data is processed; as a result, the platforms *de facto* perform tasks usually vested in public authorities.[97] To borrow Teubner's words, this framework could be described as "the constitutionalisation of a multiplicity of autonomous subsystems of world society."[98]

This situation also concerns the relationship between online platforms and public actors. Governments and public administrations usually rely on big tech companies, for example to offer new public services or improve their quality through digital and automated solutions.[99] However, this cooperation, first, leads tech companies to hold a vast amount of data coming from the public sector and, second, means that public actors increasingly depend on these companies which can impose their conditions when agreeing on partnerships or other contractual arrangements. For instance, the use of artificial intelligence by private tech companies and used by public authorities in automated decision-making in welfare programs or criminal justice is another example where the code and the accompanying infrastructure mediate individual rights.[100] This relationship affects not only principles such as transparency or fairness, but also, even more

[94] Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, Law & Pol. Econ. (Dec. 6, 2017), https://bit.ly/2K1cs3N.

[95] Emily B. Laidlaw, *A Framework for Identifying Internet Information Gatekeepers*, 24(3) Int'l Rev. L., Computers & Tech. 263 (2012); Jonathan A. Zittrain, *History of Online Gatekeeping*, 19(2) Harv. J.L. & Tech. 253 (2006).

[96] Luca Belli, Pedro A. Francisco, & Nicolo Zingales, *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, *in* How Platforms are Regulated and How They Regulate Us, *supra* note 2, at 41.

[97] Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation*, 5 Internet Pol'y Rev. (2016), https://policyreview.info/node/441/pdf; Edoardo Celeste, *Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?*, 33 Int'l Rev. L., Computers & Tech. 122 (2018).

[98] Gunther Teubner, *Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?*, *in* Constitutionalism and Transnational Governance 3 (C. Joerges, I. Sand & G. Teubner eds., 2004).

[99] For instance, smart cities are examples of this situation. *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018); Lilian Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, 1 Eur. Data Protection L. 26 (2016).

[100] Sofia Ranchordas & Catalina Goanta, *The New City Regulators: Platform and Public Values in Smart and Sharing Cities*, 36 Computer L. & Security Rev. 105375 (2020).

importantly, the principle of the rule of law, since legal norms are potentially replaced by technological and contractual standards established by private transnational actors.

Within this framework, the CJEU's judicial activism has played a crucial role in underlining the new challenges of the information society, thus paving the way to a new European constitutional phase (i.e. digital constitutionalism). As the expression suggests, digital constitutionalism has a dual nature. The first term ("digital") refers to technologies based on the Internet, such as automated technologies to process data or moderate content, whereas the second term ("constitutionalism") refers to the political ideology formulated in the eighteenth century where, according to the Lockean idea, the power of governments should be legally limited and its legitimacy dependent upon compliance with those limitations.

Despite the temporal gap between eighteenth-century constitutionalism and twenty-first-century technology, the adjective "digital" implies the collocation of constitutionalism in a temporal and material dimension. Digital constitutionalism refers to a specific timeframe evolving in the wake of the global diffusion of the web in the 1990s. Moreover, from a material perspective, this adjective leads to focusing on how digital technologies and constitutionalism affect one another. Therefore, the merging of the expressions "digital" and "constitutionalism" leads to a new theoretical and practical field based on a dynamic dialectic between how digital technologies affect the evolution of constitutionalism and the reaction of constitutional law against the power emerging from digital technologies implemented by public and private actors. As stressed by Suzor, the project of digital constitutionalism is "to rethink how the exercise of power ought to be limited (made legitimate) in the digital age."[101]

The characteristics of this new constitutional phase in the EU are based, first, on the codification of the CJEU's efforts to protect fundamental rights in the information society and, second, on the limitation of online platforms' powers through the implementation of legal instruments aimed at increasing the degree of transparency and accountability in online content moderation and data processing. Both of these characteristics can be found in the DSM strategy.[102]

Notwithstanding the fact that the implementation of new digital technologies by public actors raises serious concerns, the rise of digital constitutionalism in the EU has been primarily driven by the role of transnational online platforms, which, although vested as private actors, increasingly carry out quasi-public tasks. As the European Commission underscored, online platforms should "protect core values" and increase "transparency and fairness for maintaining user trust and safeguarding innovation."[103] The role of online platforms in the digital environment implies "wider

[101] Nicolas Suzor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, 4 Soc. Media + Soc'y (2018), https://bit.ly/37mMZKT.

[102] 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) 192 final (May 6, 2015).

[103] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016) 288 final (May 25, 2016).

responsibility."[104] Likewise, the Council of Europe has emphasized, on the one hand, the member states' positive obligation to ensure the respect of human rights and, on the other hand, the role and responsibility of online intermediaries in managing content and processing data.[105] As observed, "the power of such intermediaries as protagonists of online expression makes it imperative to clarify their role and impact on human rights, as well as their corresponding duties and responsibilities."[106]

This political statement has been supported by a new wave of soft-law and hard-law instruments aimed to regulate online intermediaries' activities in the field of content and data by introducing new obligations and users' rights. In this respect, the rise of new rights in the digital environment is not just a ("top-down") process stemming from legal institutionalization but a ("bottom-up") social need in the algorithmic society. As in other fields, such as net neutrality or the right to Internet access, new safeguards constitute the expressions of key values of the contemporary society.[107] The Directive on copyright in the DSM ("Copyright Directive"),[108] the proposal for regulation to tackle online terrorist content ("Regulation on Terrorist Content"),[109] and the adoption of the GDPR are just three examples demonstrating how the European constitutional approach aims to protect fundamental rights and democratic values while limiting the private power of online platforms.

4.1. Content: Regulating online content moderation

Within the framework of the DSM strategy, the Commission has launched (and adopted) legislative proposals to limit online platforms' discretion and increase the degree of transparency and accountability in content moderation.[110]

The first example is the adoption of the Copyright Directive which, for the first time in almost twenty years, introduced a new framework of liability for online content-sharing service providers.[111] This step can be considered a watershed, acknowledging

[104] *Id.*

[105] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, sec. 6 (Mar. 7, 2018), https://bit.ly/3mwKY3e.

[106] *Id.* sec. 7.

[107] Christoph B. Graber, *Bottom-Up Constitutionalism: The Case of Net Neutrality*, 7 Transnat'l Legal Theory 524 (2017).

[108] 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 O.J. (L 130) 92.

[109] European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM(2018)0640—C8-0405/2018—2018/0331(COD) [hereinafter Regulation on Terrorist Content].

[110] Giovanni De Gregorio, *Expressions on Platforms: Freedom of Expression and ISP liability in the Digital Single Market*, 3 Eur. Competition & Regulatory L. Rev. 213 (2018).

[111] Martin Husovec, *How Europe Wants to Redefine Global Online Copyright Enforcement*, *in* Pluralism or Universalism in International Copyright Law 513 (Tatiana E. Synodinou ed., 2019); Giancarlo Frosio & Sunimal Mendis, *Monitoring and Filtering: European Reform or Global Trend?*, *in* The Oxford Handbook of Online Intermediary Liability 544 (Giancarlo Frosio ed., 2019).

that the role of some online platforms (e.g., social media) can no longer be considered to be merely passive. Since rightsholders bear financial losses due to the quantity of copyright-protected works uploaded onto online platforms without prior authorization, the Copyright Directive establishes, inter alia, a licensing system between online platforms and rightsholders.[112] Article 17 establishes that online content-sharing service providers perform an act of communication to the public when hosting third-party content and, as a result, they are required to obtain licenses from rightsholders. If no authorization is granted, online content-sharing service providers can be held liable for unauthorized acts of communication to the public, including making available to the public copyright-protected works, unless they comply with the new exception of liability.[113]

The Copyright Directive also shows its inheritance of CJEU rulings in terms of proportionality in the field of online intermediaries' duties. The liability of online content-sharing service providers should be assessed based on "the type, the audience and the size of the service and the type of works or other subject-matter uploaded by the users of the service; and the availability of suitable and effective means and their cost for service providers."[114] Moreover, this regime partially applies to online content-sharing service providers whose services have been available to the public in the EU for less than three years and that have an annual turnover below €10 million.[115] Furthermore, the cooperation between rightsholders and online platforms should not lead to any general monitoring obligations pursuant to the decisions of the CJEU in *Scarlet* and *Netlog*.[116]

This new system of liability is not the sole novelty. The EU has not only codified the findings of the CJEU but has reached another turning point in its (digital) constitutional approach: it has limited the power of online platforms by introducing due-process safeguards in content moderation. For instance, online content-sharing service providers are required to implement an effective and expeditious complaint and make a redress mechanism available to the users of their services in the event of a dispute over the disabling of access to, or the removal of, works or other user-uploaded content.[117] These complaints have to be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review.

Likewise, the proposal for a Regulation on Terrorist Content aims to establish a clear and harmonized legal framework to tackle the misuse of hosting services for the dissemination of this type of content.[118] First, the proposal defines terrorist content.[119] As a result, since the definition is provided by law, online platforms discretion would

[112] Directive (EU) 2019/790, *supra* note 109, art. 2(6).
[113] *Id.* art. 17.
[114] *Id.* art. 17(5).
[115] *Id.* art. 17(6).
[116] *Id.* art. 17(8).
[117] *Id.* art. 17(9).
[118] Joris van Hoboken, *The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications*, Transatlantic Working Group on Content Moderation Online and Freedom of Expression (May 3, 2019), https://bit.ly/3r6feFi; Joan Barata, *New EU Proposal on the Prevention of Terrorist Content Online*, CIS Stanford Law (Oct. 2018), https://stanford.io/37n4nPw.
[119] Regulation on Terrorist Content, *supra* note 110, art. 2(1)(5).

be bound by this legal definition when moderating terrorist content. Second, hosting service providers (or online platforms) are required to act in a diligent, proportionate, and non-discriminatory manner and considering "in all circumstances" fundamental rights of the users, especially freedom of expression.[120]

Despite the relevance of these obligations, the implementation of these measures, described as "duties of care,"[121] should not lead online platforms to generally monitor the information they transmit or store, nor to a general duty to actively seek out facts or circumstances indicating illegal activity. In any case, unlike the Copyright Directive, the Regulation on Terrorist Content does not prejudice the application of the safe harbor regime established by the e-Commerce Directive. Hosting providers are only required to inform the competent authorities and expeditiously remove the content of which they became aware. In addition, online platforms are obliged to remove content within one hour of the receipt of a removal order from the competent authority.[122]

Even in this case, the EU has tried to inject procedural safeguards, requiring online platforms, for example, to set out clearly in their terms and conditions their policy on preventing the dissemination of terrorist content.[123] As a general rule, online platforms should protect their services against the public dissemination of terrorist content by adopting effective, targeted, and proportionate measures, "paying particular attention to [. . .] the fundamental rights of the users, and the fundamental importance of the right to freedom of expression and the freedom to receive and impart information and ideas in an open and democratic society."[124] Transparency obligations are not the only safeguards. Where hosting service providers use automated tools in respect of the content they store, online platforms are obliged to set and implement "effective and appropriate safeguards" ensuring that content moderation is accurate and well founded (e.g. human oversight).[125] Furthermore, it recognizes the right to an effective remedy requiring online platforms to put in place effective remedies for content providers whose content has been removed, or access to which has been disabled, following a removal order.[126]

These two examples show how the Union has, on the one hand, codified the lessons of the CJEU in terms of proportionality and, on the other hand, fostered its digital constitutional approach by limiting the discretion of online platforms in the field of content moderation. This observation should not lead to examining the European approach to online platforms just from a hard law perspective. The Commission has introduced codes of conducts and guidelines to nudge online platforms to introduce transparency and accountability mechanisms.[127] The Recommendation on

[120] *Id.* art. 3.
[121] *Id.*
[122] *Id.* art. 4(3).
[123] *Id.* art. 8(1).
[124] *Id.* art. 6.
[125] *Id.* art. 9(2).
[126] *Id.* arts 9(a)–11.
[127] European Commission, Code of Conduct on Countering Illegal Hate Speech Online (Mar. 18 2019), https://bit.ly/2WmFZYg; European Commission, Code of Practice on Disinformation (Sept. 26, 2018), https://bit.ly/2WnIcCI; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM(2017) 555 final (Sept. 28, 2017).

measures to effectively tackle illegal content online proposes a general framework of safeguards in content moderation.[128] Without being exhaustive, the Recommendation encourages platforms to publish, in a clear, easily understandable, and sufficiently detailed manner, the criteria according to which they manage the removal of, or blocking of access to, online content.[129] In the case of the removal of, or blocking of access to, the signaled online content, platforms should, without undue delay, inform users about the decision, stating their reasoning as well as the possibility to contest the decision.[130] The content provider should offer a possibility to contest the removal decision by submitting a "counter-notice" within a "reasonable period of time." The Recommendation in question can be considered a manifesto of the new approach to online content moderation in the DSM. This new set of rights, developed on the new characteristics of digital constitutionalism, aims to reduce the asymmetry between individuals and private actors implementing algorithmic technologies.

Despite the step forward made in the last years at the European level, this supranational approach has not prevented member states from following their path in the field of content moderation, especially when looking at the law introduced by Germany in the field of hate speech,[131] and France concerning disinformation.[132] In the German case, as of 2017, the Network Enforcement Act requires social media receiving more than 100 reports of illegal content in a calendar year to submit a biannual report on their content-moderation activities.[133] Even more importantly, this German law introduces a procedure to manage complaints regarding illegal content.[134] Among the obligations, social media have to remove, or block access to, content that is manifestly unlawful within twenty-four hours of receiving the complaint. In addition, social media are required to remove or block a specific content within seven days of receiving the complaint, with some exceptions.[135] Failure to comply with the provisions of this law can lead to fines of up to €50 million.[136]

[128] Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C(18) 1177 final.

[129] *Id.* at 16.

[130] *Id.* at 9.

[131] Gesetz zur Verbesserung der Rechtsdurchsetzung in Sozialen Netzwerken [NetzDG] [Act to Improve Enforcement of the Law in Social Networks], Sept. 1, 2017, BGBl at 3352 (Ger.).

[132] Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [Organic law No. 2018-1201 of 22 December 2018 on measures to combat tampering with information], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Dec. 23, 2018, n. 297; Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [Law No. 2018-1202 of 22 December 2018 on measures to combat tampering with information], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Dec. 23, 2018, n. 297 (Fr.).

[133] Thomas Wischmeyer, *What is Illegal Offline Is Also Illegal Online: The German Network Enforcement Act 2017*, *in* Fundamental Rights Protection Online: The Future Regulation of Intermediaries 28 (Bilyana Petkova & Tuomas Ojanen eds., 2019).

[134] NetzDG, BGBl at 3352, art. 3.

[135] *Id.* art. 1(3).

[136] *Id.* art. 4.

Although the EU has made some important steps forward in the field of content moderation, the legal fragmentation of guarantees and remedies at the supranational and domestic level could undermine its attempt to provide a common framework to address the cross-border challenges raised by online platforms with respect to content. In other words, if the "power of positive thinking" has led the EU to introduce significant transparency and accountability safeguards,[137] the mix of supranational and national initiatives has resulted in a decrease in the effective degree of protection for individuals and in undermining of fundamental freedoms and rights in the internal market, thereby challenging the role of digital constitutionalism in protecting individual fundamental rights and limiting the powers of online platforms. For this reason, the Digital Services Act will play a critical role in articulating the next steps of European digital constitutionalism.[138] This legal package promises to tackle the challenges of content moderation with a comprehensive approach to increase transparency and accountability while limiting the online platforms' hold on online content.

4.2. Data: The General Data Protection Regulation

The constitutional path toward protection of personal data has reached a new level, not only in the wake of the Lisbon Treaty, thanks to the role of the CJEU, but also with the adoption of the GDPR. The new European constitutional approach can be understood when comparing the first recitals of the GDPR with the Data Protection Directive. The GDPR underlines the central role of data subjects' fundamental rights within the framework of European data protection law[139] as also resulting from the case law of the CJEU in the field of digital privacy.

In order to achieve the objective of data protection without neglectIng the need to protect other constitutional interests clashing with the right to privacy and data protection,[140] the entire structure of the GDPR is based on general principles which orbit around the accountability of the data controller.[141] Even when the data controller is not established in the EU according to some conditions,[142] the GDPR increases the responsibility of the data controller which, instead of focusing on merely complying with data protection law, is required to design and monitor data processing by assessing theOrisk for data subjects' rights and freedoms.[143] In other words, even in this field, the approach of the EU aims to move from formal compliance as legal shields to substantive responsibilities (or accountability) of the data controller whose beacon are

[137] Aleksandra Kuczerawy, *The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*, 8 J. Intell. Prop., Info. Tech. & e- Commerce L. 226 (2017).

[138] Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final (Feb. 15, 2020).

[139] GDPR, *supra* note 46, recitals 1–2.

[140] *Id.* recital 4.

[141] *Id.* art. 5.

[142] *Id.* art. 3(2).

[143] Raphaël Gellert, The Risk-Based Approach to Data Protection (2020); Claudia Quelle, *The Risk Revolution in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too*, 9 Eur. J. Risk Reg. 502 (2018).

the principles of the GDPR as an expression of the fundamental rights of privacy and data protection.

Within this framework, the GDPR adopts a dynamic definition of the data controller's responsibility that considers the nature, the scope of application, the context, and the purposes of the processing, as well as the risks to the individuals' rights and freedoms.[144] On this basis, the data controller is required to implement appropriate technical and organizational measures to guarantee, and be able to demonstrate, that the processing is conducted in accordance with the GDPR. The principles of privacy by design and by default contribute to achieving this purpose by imposing an *ex-ante* assessment of compliance with the GDPR and, by extension, with the protection of the fundamental right to data protection.[145] Put another way, the GDPR focuses on promoting a proactive, rather than reactive, approach based on the assessment of the risks and on the context of specific processing of personal data. A paradigmatic example of this shift is the obligation for the data controller to carry out data protection impact assessment, which explicitly aims to also address the risks deriving from automated processing "on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."[146] This obligation requires that data controllers conduct risk assessment which is not only based on business interests but also on data subjects' (fundamental) rights and freedoms.

The GDPR has not only increased the degree of accountability of the data controller but also empowered individuals by introducing new rights of data subjects. This approach demonstrates the intent of the EU to ensure individuals are not marginalized vis-à-vis the data controller, particularly when the latter processes vast amounts of data and information through the use of artificial intelligence technologies. Among these safeguards, the GDPR establishes the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[147] This new safeguard can be considered an example of the EU reaction to the challenges raised by artificial intelligence technologies. This provision has been interpreted more as a liberty or a general prohibition, than a right of the data subject.[148] Therefore, the data subject does not need to adopt any positive conduct to rely on this right; the data controller is thus required to avoid interference with this right as if it were a negative liberty.

Like in the field of content, the GDPR aims to protect data subjects against automated decision-making processes by complementing this liberty with a positive dimension based on procedural safeguard consisting of the obligation for data controllers to implement "at least" the possibility for the data subject to obtain human intervention,

[144] GDPR, *supra* note 46, art. 24.

[145] *Id.* art. 25.

[146] *Id.* art. 35(3)(a).

[147] Sandra Wachter & Brendt Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 Colum. Bus. L. Rev. 494 (2019).

[148] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Doc. wp251rev.01 (rev'd Feb. 6, 2018), https://bit.ly/386ddQW.

express his or her point of view, and contest decisions.[149] Recital 71 specifies that the processing should be subject to suitable safeguards, including "specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision." The provision of the "human intervention" as a minimum standard in automated processing would foster the role of data subjects in the algorithmic society. In other words, this right aims to increase the degree of transparency and accountability for individuals which can rely on their right to receive information about automated decisions involving them.

This provision has sparked a debate among scholars on whether the GDPR provides effective grounds to protect from potentially harmful consequences of automated decision-making processes, most notably by creating a "right to explanation."[150] Some scholars argue that the GDPR fosters qualified transparency over algorithmic decision-making.[151] In contrast, others support or question the existence of a right to explanation,[152] or doubt that the GDPR offers a concrete remedy to algorithmic decision-making processes.[153] Despite different views, this right of the data subject does not overcome the new challenges posed by the algorithmic society. First, it should not be neglected that enhancing due-process safeguards could affect the freedom to conduct business or the performance of a public task, due to additional human and financial resources required to adapt automated technologies to the data protection legal framework. Second, the presence of a human being does not eliminate the risks of error or discrimination. Third, the opacity of some algorithmic processes could not allow the data controller to provide the same degree of explanation in any case.

Nevertheless, this provision, together with the principle of accountability, constitutes a crucial step in the governance of automated decision-making processes.[154] From a constitutional perspective, Article 22 provides a safeguard against the massive spread of artificial intelligence technologies promising to replace humans in decision-making activities and increasingly affecting the rights of individuals. Since automated systems are developed according to the choice of programmers who, by setting the rules of technologies, transform legal language in technical norms, they contribute to defining transnational standards of protection outside the traditional channels of democratic control. This situation not only raises threats for the principles of European

[149] GDPR, *supra* note 46, art. 22(3).

[150] *See* Bryce Goodman & Set Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation,"* 38 AI Mag. 50 (2017); Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7(4) Int'l Data Privacy L. 233 (2017). Maya Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, 27(2) Int. J. Law Info. Tech. 91 (2019).

[151] Margot E. Kaminski, *The Right to Explanation, Explained*, 34(1) Berkeley Tech. L.J. (2019).

[152] Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(4) Int'l Data Privacy L. 76 (2017); Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7(4) Int'l Data Privacy L. 243 (2017).

[153] Lilian Edwards & Michael Veale, *Slave to The Algorithm? Why a "Right to an Explanation" Is Probably not the Remedy You Are Looking for*, 16 Duke L. & Tech. Rev. 18 (2017).

[154] Margot Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529 (2019).

data protection law, but, even more importantly, challenges the principle of the rule of law since, even in this case, legal norms are potentially replaced by technological standards outside any democratic check or procedure.

The GDPR has not provided a comprehensive answer to these challenges or, more generally, to the fallacies of European data protection law.[155] Without being exhaustive, it is worth underlining how the potential scope of the principle of accountability leaves data controllers to enjoy margins of discretions in deciding what degree of safeguards are sufficient to protect the fundamental rights of data subjects in a specific context. In other words, the risk-based approach introduced by the GDPR appears to delegate to the data controller the power to balance conflicting interests, thus making the controller the "arbiter" of data protection. Although the GDPR can no longer be considered the panacea coming from European digital constitutionalism, it constitutes an important step forward in the field of data protection. As it did in the case of content, the EU approach has focused its efforts on limiting discretion in the use of algorithmic technologies and empowering data subjects by granting them new rights in the algorithmic society in light of the constitutional protection ensured by Articles 7 and 8 of the EU Charter.

5. Toward a fourth phase in a global context?

The EU approach to the digital environment has evolved in the last twenty years. This change of paradigm offers clues to understanding the reasons for the rise of European digital constitutionalism, showing why the EU has complemented liberal goals with a new (digital) constitutional strategy. The liberal narrative characterizing the EU's policy at the beginning of this century has slowly faded away. While promoting the development of digital services has played a crucial role in the development of the internal market, a liberal approach in this field has also contributed to undermining individuals' fundamental rights and freedoms, while allowing private actors to consolidate newly found powers. The phase of judicial activism has been the first reaction against this situation, and it has paved the way for European digital constitutionalism. In order to counteract a phase of legislative inertia, the CJEU has underscored the role of fundamental rights in the digital environment by increasingly acting like a quasi-constitutional court. This second phase has just been a transition anticipating a new phase of European (digital) constitutionalism. The codification of the CJEU's efforts and the limitation of online platforms' discretion are the first steps in the third phase of European policy opposing the troubling rise and evolution of private powers in the algorithmic society.

Despite the aforementioned challenges, the EU has not introduced provisions to censor online content or prohibit the use of some technologies to process data. The European strategy has focused on introducing safeguards to foster transparency and accountability in online content moderation and data processing. The rise of European

[155] Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 Int'l Data Privacy L. 250 (2014).

digital constitutionalism has not led to a dangerous escalation of authoritarian reaction, but regulatory solutions to protect fundamental rights and democratic values in a context that is very unlike the digital environment at the end of the last century. The possibility for individuals to obtain justification for automated outcomes, access redress mechanisms, or human intervention would mitigate the gap between humans and machines, individuals and powers. Put differently, these new rights would allow users to rely on a (first) "human translation" of the algorithmic process. As Pasquale explained,

> [W]ithout knowing what Google actually does when it ranks sites, we cannot assess when it is acting in good faith to help users, and when it is biasing results to favor its commercial interests. The same goes for status updates on Facebook, trending topics on Twitter, and even network management practices at telephone and cable companies.[156]

These new safeguards would increase transparency and accountability, thus fostering (technological) due process.[157]

In this scenario, the rise of European digital constitutionalism represents the end of the liberal EU approach and a potential basis for promoting a democratic digital environment in the EU. However, digital constitutionalism seems to be far from the last step on the EU's regulatory path. It might be already possible to outline a new evolving trend in EU policy, characterized by the extension of constitutional values beyond EU borders and the articulation of a human-centric technological model.

In the field of content, the provisions established by the Copyright Directive and the proposal for a Regulation on Terrorist Content and the Digital Services Act would require transnational corporations to comply with new obligations concerning content moderation. This approach could spread democratic views on freedom of expression around the globe, since online platforms would be encouraged to set the degree of protection required by EU law as a general standard in order to avoid the financial and organizational burden resulting from the adoption of different models of content moderation. However, this approach would also clash with different constitutional and legal traditions of other countries. The *Glawischnig-Piesczek* case helps sketch this scenario.[158] In this case, the applicant sought a judicial order requiring Facebook to cease publication of "identical" or "equivalent content" on a global scale. The CJEU recognized that the e-Commerce Directive does not preclude the global scope of the measures which member states are entitled to adopt.[159] According to the CJEU, "in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level."[160] As a result, the CJEU ruled that EU law does not preclude a

[156] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 9 (2015).

[157] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014); Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Danielle K. Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008).

[158] Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, ECLI:EU:C:2019:821 (Oct. 3, 2019).

[159] *Id.* at 49–50.

[160] *Id.* at 51.

national court from ordering the removal of information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law. It is up to member states to take that law into account.[161]

In the field of data, the potential extension of European constitutional values is even more evident.[162] If, in the *Schrems* saga, the CJEU has already shown the ability of European data protection law to extend its scope of application overseas, the adoption of the GDPR would have confirmed this trend by apparently extending the paradigm of the protection of personal data to the global context. The scope of the application of the GDPR is also the result of several judicial attempts by the CJEU to ensure the effective protection of the rights of EU citizens beyond its borders.[163] Indeed, the GDPR not only ensures that European data protection law applies to the "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not",[164] it also completes this framework by adding that, even though the controller is established outside the EU, the GDPR is nevertheless applicable if the processing of personal data consists of the provision of products or services to individuals residing in the Union or the targeting of consumers' behavior.[165] This provision can be considered the result of a high-level constitutional standard of protection in Europe, which, in the information society, can no longer be limited to the EU territory in order to ensure that natural persons are not deprived of the protection to which they are entitled.[166]

The consequence of such a rule is twofold. On the one hand, this provision involves jurisdiction. The GDPR's territorial scope of application overrides the doctrine of establishment developed by CJEU case law, since even those entities that are not established in the EU will be subject to the GDPR. On the other hand, the primary consequence of such an extension of territoriality is to extend EU constitutional values to the global context. Scholars have already discussed the "long arm of EU data protection law" within the framework of the Data Protection Directive,[167] the "global reach of EU law,"[168] or, more generally, the "Brussel effect" to describe the power of the European Union to export its policy worldwide.[169]

[161] Lorna Woods, *Facebook's Liability for Defamatory Posts: The CJEU Interprets the E-Commerce Directive*, EU Law Analysis Blog (Oct. 7, 2019), https://bit.ly/2Wjpj3M.

[162] Christoper Kuner, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, 5 Int'l Data Privacy L. 23 (2015).

[163] C-131/12, Google Spain, 2014, ECLI:EU:C:2014:317; Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639 (Oct. 1, 2015).

[164] GDPR, *supra* note 46, art. 3(1).

[165] *Id.* art. 3(2).

[166] *Id.* recital 23. *See also* Oreste Pollicino, *Data Protection and Freedom of Expression Beyond EU Borders: EU Judicial Perspectives*, *in* Data Protection beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty 81 (Federico Fabbrini, Edoardo Celeste, & John Quinn eds., 2020).

[167] Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 Int'l Data Privacy L. 28 (2018).

[168] Christopher Kuner, *The Internet and the Global Reach of EU Law*, *in* EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law 112 (Marise Cremona & Joanne Scott eds., 2019).

[169] Anu Bradford, *The Brussel Effect*, 107 Nw. U. L. Rev. 1 (2015). See also the position of Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 Am. J. Comp. L. 87 (2014).

Nevertheless, the extension of data protection rules to the global context could also have some drawbacks. The scope of their application could affect legal certainty, with troubling results not only for the internal market but also for general principles such as the rule of law. As already observed:

> [W]hen a law is applicable extraterritorially, the individual risks being caught in a network of different, sometimes conflicting legal rules requiring simultaneous adherence. The result—conflicts of jurisdiction—may put an excessive burden on the individual, confuse him or her, and undermine the individual's respect for judicial proceedings and create loss of confidence in the validity of law.[170]

Furthermore, the far-reaching scope of European constitutional values could affect the right to freedom of expression and financial interests of other countries and their citizens.[171] This approach would promote a vision of "privacy universalism."[172] The CJEU has recently highlighted these challenges in the *Google v. CNIL* decision, where the core of the preliminary questions raised by the French judge aimed to clarify the territorial boundaries of the right to be forgotten online.[173] According to the CJEU, on the one hand, search engines organize information into a list of results based, for example, on a thorough search for an individual's name, thus justifying "the existence of a competence on the part of the EU legislature to lay down the obligation, for a search engine operator, to carry out, when granting a request for de-referencing made by such a person, a de-referencing on all the versions of its search engine."[174] On the other hand, the right to the protection of personal data is not an absolute right, but must be balanced with other fundamental rights in relation to its function in society and in accordance with the principle of proportionality.[175] Therefore, a global delisting would extend European constitutional values also to third states which do not recognize the right to delisting or the same degree of protection to the right of freedom of expression.

This trend seems to suggest how the EU aims less to extend constitutional values beyond its territorial borders than to avoid having online platforms formally rely on their geographical location (i.e. establishment) as a shield to avoid compliance with EU law. If, on the one hand, the EU aims to avoid that the cross-border nature of the digital environment can be used as a competitive advantage affecting competition in the internal market, on the other hand, even more importantly, the protection of fundamental rights in a global context should take into consideration that other countries are still following a (digital) liberal approach like the United States, at least at the federal level, or playing a

[170] Paul De Hert & Michal Czerniawski, *Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context*, 6 Int'l Data Privacy L. 230, 240 (2016).

[171] Dan J. B. Svantesson, *A "Layered Approach" to the Extraterritoriality of Data Privacy Laws*, 3 Int'l Data Privacy L. 278 (2013).

[172] Payal Arora, *GDPR: A Global Standard? Privacy Futures, Digital Activism and Surveillance Cultures in the Global South*, 17 Surveillance & Soc'y 717 (2019).

[173] Case C-507/17, Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019).

[174] *Id.* at 58.

[175] *Id.* at 60. *See also* Cases C-92/09 & C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 2010 E.C.R. I-11063, at 48; Opinion 1/15 (EU–Canada PNR Agreement) July 26, 2017, at 136.

predominant role in the rush for the primacy over artificial intelligence technologies like China. In other words, rather than a "European data privacy imperialism,"[176] a potential fourth phase leading to the consolidation of European digital constitutionalism would lead to a new phase of transnational constitutional law whose aim is to protect fundamental rights and democratic values in the algorithmic society.

The Union has shown its intention to deal with the challenges raised by private powers in the age of artificial intelligence.[177] According to Vestager,

> [T]here's no doubt, in other words, that platforms—and the algorithms they use—can have an enormous impact on the way we see the world around us. And that's a serious challenge for our democracy. [. . .] So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms.[178]

The High-Level Expert Group on Artificial Intelligence proposed a anthropocentric approach for all automated systems.[179] The European Data Protection Supervisor, too, stressed that: "[The] respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics."[180]

These statements should not surprise, but rather underscore one of the essential peculiarities of European constitutionalism which is rooted in human dignity.[181] Against the potential trend that would replace human beings with automated technologies, the European Union's approach can rely on a constitutional foundation in addressing the threats posed by ubiquitous automation that takes individuals out of the equation. While the rise of European digital constitutionalism has shown constitutional law's resilience in the face of threats to fundamental rights, posed by the exercise of private powers in the information society, a fourth phase, or better a more sophisticated articulation of European digital constitutionalism, would focus on addressing the new threats to human dignity (i.e. digital humanism). This new phase should not be seen merely as an imperialist extension of constitutional values outside the EU territory but as a reaction of European constitutionalism to the challenges to human dignity in an algorithmic society. In this scenario, the evolution of European digital constitutionalism would oppose techno-determinist solutions and contribute to promoting the European model as a sustainable constitutional environment for the development of artificial intelligence technologies in the global context.

[176] Svantesson, *supra* note 172, at 279.

[177] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *On the European democracy action plan*, COM(2020) 790 final (Dec. 3, 2020); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Shaping Europe's digital future*, COM(2020) 67 final (Feb. 19, 2020). *See also On Artificial Intelligence: A European Approach to Excellence and Trust*, COM(2020) 65 final (Feb. 19, 2020).

[178] Margrethe Vestager, *Algorithms and Democracy*, AlgorithmWatch Online Policy Dialogue (Oct. 30, 2020), https://bit.ly/2X3gpHT.

[179] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (Apr. 8, 2019), https://bit.ly/2WjNWgE.

[180] European Data Protection Supervisor, *Opinion 4/2015, Towards a New Digital Ethics* (Sept. 11, 2015), https://bit.ly/38Y4Nf3.

[181] Catherine Dupré, The Age of Dignity Human Rights and Constitutionalism in Europe (2016).