The Rise of Digital Constitutionalism in the European Union

Giovanni De Gregorio

Abstract: In the last twenty years, the EU policy in the field of digital technologies has shifted from a liberal economic perspective to a constitutional-based approach. The development of digital technologies has not only challenged the protection of individuals' fundamental rights such as freedom of expression and data protection. Even more importantly, this new technological framework has also empowered transnational corporations operating in the digital environment as hosting providers to perform quasi-public functions in the transnational context. These two drivers have led the Union to enter into a new phase of modern constitutionalism (ie digital constitutionalism). This evolution is described by three constitutional phases: digital liberalism, judicial activism and digital constitutionalism. At the end of the last century, the Union adopted a liberal approach. A strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were going to revolutionize the entire society and promising new opportunities for the internal marked. The end of this first season was the result of the emergence of the Nice Charter as a bill of rights and new challenges raised by private actors in the digital environment. In this phase, the ECJ has played a pivotal role in moving the EU standpoint from fundamental freedoms to fundamental rights. This second phase has only anticipated a new season of constitutionalism based on codifying of the ECJ's case law and limiting online platforms' powers within the framework of the Digital Single Market. The path of digital constitutionalism is still at the beginning. A fourth phase of EU constitutionalism is around the corner based on the extension of constitutional values beyond EU borders and the expression of a human-centric technological model in a global context.

1. Introduction

In the last twenty years, the policy of the European Union ("EU" or "Union") in the field of digital technologies has shifted from a liberal economic perspective to a constitutional-based approach. In order to understand this change of heart, it is necessary to frame the debate within the algorithmic society, also named as "algocracy."[1] The development of digital technologies has not only challenged the protection of individuals' fundamental rights such as freedom of expression and data protection. Even more importantly, this new technological framework has also empowered transnational corporations operating in the digital environment as hosting providers

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

("online platforms") to perform quasi-public functions in the transnational context, thus, competing with public actors.

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, on the other hand, it has also led to serious interferences with fundamental rights and the rise of private powers online, thus, triggering the Union to enter a new phase of modern constitutionalism (i.e. digital constitutionalism). As a result, the debate is no longer locked into the field of private law but is shifting to a public law perspective, and more specifically, a digital constitutional one.[2] Indeed, among its role, modern constitutionalism aims to, on the one hand, to protect fundamental rights, and, on the other hand, limit the emergence of powers outside any control.[3] A new season of 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]

This evolution questions the role of constitutionalism, especially concerning the protection of fundamental rights and the limitation of powers. Constitutions have been developed with a 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 processing data and organizing content. 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.

Within this framework, this work analyzes the path (and the reasons) leading the EU policy to move a liberal to a constitutional approach concerning the digital environment in the last thirty years. The primary goal of this article is to describe the characteristics of digital constitutionalism as a new constitutional moment and outline the potential evolution of the EU policy in the global context. It aims to explain the paradigm shift from a liberal to a (digital) constitutional approach according to two perspectives: the threats to fundamental rights and the rise of private powers in

[2] Recently, scholars have approached the public role of online platforms from different perspectives. See e.g. Natali Helberger et al. *Governing Online Platforms: from Contested to Cooperative Responsibility* 34(1) THE INFORMATION SOCIETY 1 (2018); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech* 131 HARV. L. REV. 1598 (2018); Orla Lynskey, *Regulating Platform Power*, LSE LEGAL STUDIES WORKING PAPER 1 (Feb. 21, 2017) http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf; Julia E. Cohen, *Law for the Platform Economy,* 51 U.C. DAVIS L. REV. 133 (2017).

[3] Jeremy Waldron, *Constitutionalism: A Skeptical View*, NYU SCHOOL OF LAW, PUBLIC LAW RESEARCH PAPER NO. 10-87 (May 1, 2012) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1722771&rec=1&srcabs=1760963&alg=1&pos=1; 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 (Cambridge University Press, 2019), 173.

[5] Claudia Padovani & Mauro Santaniello, *Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system*, 80 INT. COMMUN. GAZ. 295 (2018).

the algorithmic society. Furthermore, this work outlines the potential evolution of digital constitutionalism underlining the role of the Union policy in a global context.

This work aims to provide a new contribution to enrich the *status quo* of the scholars' debate from at least two standpoints. Unlike other works, it focuses on describing the challenges for constitutionalism in the algorithmic society from an EU constitutional law perspective, especially by focusing on the fields of content and data.[6] Secondly, other works have primarily focused on explaining this new constitutional moment,[7] or mapping bill of rights and legislative attempts concerning the relationship between Internet and constitutions.[8] Instead, this contribution examines how the rise and consolidation of a new season of EU (digital) constitutionalism as an example of how constitutional law can react against the challenges posed by digital and automated technologies, especially where transnational private actors operating in the digital environment are involved. Although the challenges coming from the implementation of these technologies also involve public actors, this work argues that the reaction of EU constitutionalism is primarily the result of the threats to fundamental rights coming from the rise of new private powers in the algorithmic society.

In order to achieve these goals, this work focuses on three phases: digital liberalism, judicial activism and digital constitutionalism. For each phase, the fields of online content and data are analyzed as examples of the evolution of the EU policy, as also influenced by the role of the Council of Europe. The first part of this work focuses on framing the first steps taken by the Union to regulate online intermediaries and data at the end of the last century. The second part analyzes the role and efforts of the European Court of Justice ("ECJ") in underling the relevance of fundamental rights in the EU digital environment in the aftermath of the adoption of the Lisbon Treaty. The third part focuses on the phase of digital constitutionalism in the framework of the European Digital Single Market ("DSM") strategy. The last part describes the primary findings of this work and underlines the potential evolution of digital constitutionalism in the global context.

2. The First Phase: Digital Liberalism

Following the signing of the Treaty of Rome in 1955, 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 EU in the field of digital technologies. Until the adoption of the Nice Charter in

[6] For an Australian perspective, see Monique Mann, *The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance In Australia*, 80 INT. COMMUN. GAZ. 369 (2018).
[7] Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorization*, 33(1) IRLCT 76 (2019).
[8] Dennis Redeker et al., *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 80 INT. COMMUN. GAZ. 302 (2018); Mauro Santaniello et al., *The Language of Digital Constitutionalism and the Role of National Parliaments*, 80 INT. COMMUN. GAZ. 320 (2018).
[9] 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).

2000 ("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]

This liberal approach was indeed transposed in the regulation of the digital environment. In the field of data and content, it would be sufficient to take as examples the Directive 95/46/EC ("Data Protection Directive") and Directive 2000/31/EC ("e-Commerce Directive") to understand that the policy goal of the Union oriented to ensure the smooth development of the internal market.[12]

Such a liberal approach should not be surprising if it is framed within the debate about Internet regulation at the end of the last century where the online environment was considered an area outside public actors' interference.[13] In the "Declaration of Independence of Cyberspace,"[14] 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."[15] This independent world from physical location was also supported by Johnson and Post,[16] who consider a "decentralised and emergent law", resulting from customary or collective private action, the basis for creating a democratic set of rules applicable to the digital community.[17] In other words, these ideas are based on a bottom-up approach: rather than relying on traditional public law-making 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.[18]

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 tries to cut the heads of the mythical beast, other ones grow up. The same parallelism occurs when regulators attempt to interfere with the online environment (cutting one head off the Hydra) and users easily circumvent the new rules (the growth of new heads).

---

[10] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[11] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, Title II and IV.

[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] OJ L 281/31; 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] OJ L 178/1.

[13] Among the most relevant scholars, see John Perry Barlow, David Johnson, David Post and Tom W. Bell.

[14] John P. Barlow, *A Declaration of Independence of the Cyberspace*, ELECTRONIC FRONTIER FOUNDATION 1996) www.eff.org/cyberspace-independence.

[15] *Id.*

[16] David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48(5) STAN. L. REV. 1367, 1371 (1996).

[17] David R. Johnson & David Post, *And How Shall the Net be Governed?*, in COORDINATING THE INTERNET (Brian Kahin and James Keller eds, 1997).

[18] The democratic development of a set of rules related to the digital space has been criticized due to lack of a unique community in the digital environment. See CASS SUNSTEIN, REPUBLIC 2.0 (Princeton University Press 2009). Moreover, Reed recognized that, although the interpretation of the digital space by the Cyberlibertarian doctrine is not entirely wrong, the weak point depends on the physical substance of the individual that acts in the digital environment. See CHRIS REED, INTERNET LAW: TEXT AND MATERIALS 174-5 (Cambridge University Press, 2007).

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

This metaphor implicitly demonstrates not only the trade-off 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 toward 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 rather than on the protection of individuals' rights and freedoms. A strict 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, in the aftermath of the Internet, the EU approach was comprehensively far from digital constitutionalism because new digital technologies were considered as an opportunity to grow and prosper. At that time, there were no reasons to fear the rise of new private powers challenging the protection of fundamental rights online and competing with States' powers.

Within this framework, this section analyzes how this liberal framework has characterized the Union 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: e-Commerce Directive

The adoption of the e-Commerce Directive can be considered one of the first examples of the EU liberal approach concerning the digital environment. 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]

Within this framework, the e-Commerce Directive establishes a regime of exemption of liability for internet service providers (or "online intermediaries"). Based on the US "safe harbor" model introduced at the end of the last century by the Communication Decency Act,[22] and the Digital Millennium Copyright Act,[23] this regime acknowledges the non-involvement of online intermediaries in the creation of content, thus, exempting them from liability for transmitting or hosting unlawful third-party content.[24]

When the US Congress passed Section 230 of the Communication Decency Act in 1996, the primary aim was to encourage free expression and development of the digital environment.[25] In order to achieve this objective, the choice was to exempt 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

[20] Governments have not adopted the same free-market approach concerning the internet like China and the Arab states. See Barney Warf, *Geographies of Global Internet Censorship*, 76 GEOJOURNAL 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] Digital Millennium Copyright Act, 17 U.S.C. § 512.
[24] THE RESPONSIBILITIES OF ONLINE SERVICE PROVIDERS (Mariarosaria Taddeo & Luciano Floridi eds, 2017); SECONDARY LIABILITY OF INTERNET SERVICE PROVIDERS (Graeme Dinwoodie ed., 2017).
[25] Klonick, *supra* note 2.

cases concerning their liability for editing third-party content.[26] 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.[27]

Likewise, the aim of the EU liability exemption is twofold. Firstly, the e-Commerce Directive aims to foster the development of information society through the free movement of information society services as a "reflection in Community law of a more general principle, namely freedom of expression",[28] enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms ("Convention").[29] Secondly, 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.[30] 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.[31] Furthermore, among online intermediaries,[32] hosting providers are not liable for the information or content stored by their users unless, upon becoming aware of the unlawful nature of the information or content stored, they do not promptly remove or disable access to the unlawful information or content.[33]

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 organizing and moderating content through artificial intelligence technologies.

Therefore, if, on the one hand, this political choice was aimed to ensure 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' activities 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 amount of content based just 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

[26] 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).
[27] Zeran v. Am. Online, Inc. 129 F.3d 327, 330 (4th Cir. 1997).
[28] E-Commerce Directive, *supra* note 12, Recital 9.
[29] European Convention on Human Rights [1950].
[30] *Id.*, art. 15.
[31] Nevertheless, when implementing the e-Commerce Directive in their respective national legislation, Member States are free to impose on ISPs 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).
[32] This ban applies to three categories of online intermediaries: access providers, caching providers and hosting providers E-Commerce Directive, *supra* note 12, arts 12-14.
[33] *Id.*, art. 14.

even that content whose illicit nature is not fully evident (i.e. collateral censorship).[34] Indeed, this liability regime incentivizes online platforms to focus on minimizing this economic risk rather than adopt a fundamental rights-based approach. As a result, this system of liability works as a legal shield for online intermediaries,[35] and, even more importantly, it has encouraged online platforms to set their rules to organize and moderate content based on the risk of being sanctioned and other discretionary (but opaque) conditions.[36]

This incentive (or indirect delegation) to moderate content can be considered one of the primary reasons explaining how online platforms (e.g. social media) enjoy a broad margin in determining the scope of protection of fundamental rights in the digital environment. As this work explains, the turning of this freedom into a new form of power is one of the primary challenges which led to the rise of digital constitutionalism.

2.2 Data: Data Protection Directive

In the field of data, the liberal approach of the Union is counterintuitive. At first glance, the Union has not followed a liberal regulatory path. Rather than exempting online 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.[37]

The rise and consolidation of data protection law can be explained as a response to the information society driven by new technologies and, especially, automated systems implemented by public and private entities to process data. In other words, if the right to privacy was enough to meet the interests of individuals' protection,[38] in the information society, the processing of personal data has made no longer sufficient to protect only the negative dimension of the aforementioned fundamental right leading to the rise of a positive approach to increase the degree of transparency and accountability in data processing.[39]

Whilst the Council of Europe had played a crucial role in consolidating the constitutional dimension of the right to protection of personal data in Europe,[40] this consideration can be only

[34] Regarding the risk of collateral censorship, see ECHR 16 June 2015, Delfi AS v. Estonia; ECHR 2 February 2016, MTE v. Hungary. 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).

[35] Frank Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, 17 TIL 487 (2016): Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986 (2008).

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

[37] Data Protection Directive, *supra* note 12, Recital 4.

[38] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[39] Serge Gutwirth & Paul De Hert, *Regulating Profiling in a Democratic Constitutional States*, in PROFILING THE EUROPEAN CITIZEN (Mireille Hildebrandt & Serge Gutwirth eds., 2006), 271.

[40] See, in particular, Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, January 28, 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. This international legal instrument has been amended in 2018. See Council of Europe, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, May 18, 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

partially extended to the Union 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. Indeed, in 1995, the Union policy was oriented to an economic approach towards 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 the fundamental freedoms of the Union.[41] Although the Data Protection Directive highlights that the processing of personal data shall serve mankind and aim to protect the fundamental right to privacy of data subjects,[42] 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.[43]

From an ex-post perspective, both the time of adoption, at the end of the last century, and the lack of any review in more than twenty years could explain why EU data protection law has shown its fallacies before of the challenges raised by online platforms in the digital environment. At the end of the last century, the Union 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 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, since 1995, the first draft of reviewing the privacy and data protection regime has been proposed only in 2012,[44] and the General Data Protection Regulation ("GDPR") entered into force in 2016, even without any binding effect until May 2018.[45] In other words, the (digital) liberal approach of the Union in this field has resulted from an omissive approach rather than a positive one, as in the case of the e-Commerce Directive.

Moreover, the characteristics of EU Directives can explain another reason for the inadequacy of the EU 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' norms provide just the result to be achieved and are not generally applicable without domestic implementation.[46] Therefore, the Member States' margin of discretion in implementing the Data Protection Directive is another reason explaining 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 transnational challenges.

---

[41] Data Protection Directive, *supra* note 12, Recital 3.
[42] *Id.*, Recital 2.
[43] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data [1990] COM(90) 314 final.
[44] 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) [2012] COM(2012) 11 final.
[45] 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] OJ L 119/1.
[46] TFEU, *supra* note 11, art 288.

Within this framework, the liberal approach together with 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 not just the result of the liberal frame but the regulatory design and omissive approach of the Union since the adoption of the Data Protection Directive. In other words, like in the field of data, the shift from freedom to power shows why the Union approached a new (digital) constitutional strategy.

3. The Second Season: Judicial Activism

The end of the first (liberal) season can be explained by focusing on two events, which have, at the very least, triggered a new phase of judicial activism. The first event concerned the emergence of new actors in the digital environment (i.e. online platforms), whereas the second involved the increasing role of the Charter as a bill of rights of the Union.[47]

The first transformation concerns the role of online intermediaries, particularly hosting providers. At the end of the last century, these entities provide access, 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 organization or moderation of content. 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 2000. This difference can be explained by looking at the online platforms' business model which is primarily based on profits from advertising revenues. Indeed, the primary activities of such actors do not consist of providing free online spaces where users can share information and opinions. On the contrary, online platforms gain profits from advertising based on profiling users' data.[48] Here, the intimate relationship between content and data in the framework of online platforms' business 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 enforce their community rules.[49] The increasing involvement of platforms in the organization of content and the profiling of users' preferences by 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 is difficult to support.

Secondly, the recognition of the binding nature of the Charter and its inclusion in EU primary law have contributed to codifying the constitutional dimension of the EU (digital) environment.[50]

---

[47] Grainne De Burca, *After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, 20(2) MJECL 168 (2013).
[48] DIGITAL DOMINANCE: THE POWER OF GOOGLE, AMAZON, FACEBOOK, AND APPLE (Martin Moore & Damian Tambini eds., 2018).
[49] Tarleton Gillespie, CUSTODIANS OF THE INTERNET. PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA (Yale University Press 2018).
[50] Consolidated version of Treaty on the European Union, [2012] OJ C 326/13, art. 6(1).

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 Convention.[51] In particular, the Strasbourg Court has played a crucial role not only in protecting the aforementioned fundamental rights but also underlining the constitutional challenges coming from new technologies.[52]

The adoption of the Lisbon Treaty has constituted the further step in this process. Indeed, the right to freedom of expression,[53] private and family life,[54] and the protection of personal,[55] as already enshrined in the Nice Charter, have become binding vis-a-via Member States and EU institutions,[56] which can interfere with these rights only according to test established by Article 52 of the Charter.[57] Besides, the Charter adds another important piece of the EU 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."[58]

Within this new constitutional framework, the ECJ started to rely on the Charter to answer the challenges raised by the digital environment. Both in the field of content and data, the ECJ interpreted the Charter's rights and freedoms with the aim to ensure the effective protection of these constitutional interests. As the next subparagraphs show, given the lack of any legislative review of either the e-Commerce Directive or the Data Protection Directive, judicial activism has been the critical driver highlighting the challenges for fundamental rights online, thus, promoting the transition from a mere economic perspective to a new constitutional season named digital constitutionalism.

3.1 Content: From Economic Interests to Fundamental Rights

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

In the case of *Google France,*[59] the ECJ concluded that, where an Internet-referencing service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored, it cannot be held liable for the data that it has 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 failed to act expeditiously to remove or to disable access to the data concerned. The

[51] Convention, *supra* note 29, arts 8, 10.
[52] 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 ELJ 155 (2019).
[53] Charter, *supra* note 10, art 11(1).
[54] *Id*., art. 7.
[55] *Id*., art. 8(1).
[56] *Id*., art. 51.
[57] Koen Lenaerts, *Exploring the Limits of the EU Charter of Fundamental Rights*, 8(3) EUR. CONST. L. REV. 375 (2013).
[58] Charter, *supra* note 10, art 54.
[59] 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 ECR I-02417 (decided Mar. 23, 2010).

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 possibility to access the more relevant sites, "however, it does not have an interest in bringing any specific site to the internet user's attention."[60] Although the Advocate General did not recognize the active role of this provider, the liberal frame of this and opinion and the role of automated processing systems had already shown their relevance in sharing the field of online content.

A step forward was made in *L'Oréal*.[61] The Court recognized that the offering of assistance, including the optimization, presentation or promotion of the offers for sale, was not a neutral activity performed by the provider in question according to Recital 42.[62] Although the Court has not expressly recalled the opinion of Poiares Maduro in *Google France*, this decision firstly acknowledged how automated technologies have led some providers to perform an active role rather than the mere passive provisions of digital products and services.

In 2011, the ECJ shifted this approach from a merely economic perspective to a fundamental rights-based approach. It is not by chance that this turning point occurred in the aftermath of the Lisbon Treaty recognizing that the Charter has the same legal value as the Treaties. The Court, firstly, addressed two cases involving online intermediaries and, in particular, the extent of the ban on general monitoring. In *Scarlet* and *Netlog*,[63] the question concerned the prohibition Member States to impose either 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 ECJ, an injunction to install a general filtering system would not respect the freedom to conduct business of online intermediaries.[64] 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.[65] Indeed, the ECJ 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 measure; exclusively at its expense; and for an unlimited period" violated the ban on general monitoring obligation.

---

[60] Opinion of Advocate General Poiares Maduro delivered on 22 September 2009, Opinion of AG Poiares Maduro, at 144

[61] Case 324/09, L'Oréal SA and Others v. eBay International AG and Others, 2011 ECR I-06011 (decided Jul. 12, 2011). See Patrick Van Eecke, *Online service providers and liability: A plea for a balanced approach,* 48(5) COMMON MARKT. L. REV. 1455 (2011).

[62] *Id.*, at 124.

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

[64] Scarlet, *supra* note 63, at 50.

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

Since that time, the ECJ has relied on the Charter to adjudicate other cases involving online intermediaries. For example, in *Telekabel* and *Mc Fadden*,[66] the ECJ addressed two other cases involving injunction orders on online intermediaries which leave the provider free to choose the measures to tackle copyright infringements while maintaining the exemption of liability showing its duty of care in respect of EU fundamental rights. The ECJ 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 ECJ did not solve the challenges raised by online platforms, especially concerning their liability for actively organizing third-party content as well as transparency and accountability when autonomously implementing automated decision-making technologies for content moderation. As the next section shows, these systems allow platforms to perform their activities in a manner that questions not only the system of the e-Commerce Directive but also constitutional values such as the protection of fundamental rights and the rule of law. Since online platforms contribute to defining the standard of protection of rights online on a global scale, the role of digital constitutionalism aims to cope with these challenges which the ECJ has clearly underlined. As the next sections show, the Union is orienting its approach towards the regulation of content moderation through the introduction of transparency and accountability of online platforms activities.

3.2 Data: The Judicial Path towards Digital Privacy

The role of the ECJ has not only contributed to increasing the degree of fundamental rights' protection in relation to online content but also consolidating and emancipating the right to data protection in the EU framework.[67] As in the case of online content, the recognition of the Charter as a primary source of EU law and the increasing relevance of data in the information society have encouraged the ECJ to go beyond the economic-functional dimension of the Data Protection Directive to a constitutional approach, as the decisions on digital privacy demonstrate in the aftermath of the Lisbon Treaty. As a first step, in the *Promusicae* case,[68] the Court has recognized the relevance of data protection "namely the right that guarantees protection of personal data and hence of private life,"[69] despite its functional link with the protection of privacy.[70]

[66] Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, 2014 (decided Mar. 27, 2014); Case C-484/14, Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, 2016 (decided Sept. 15, 2016). See Martin Husovec, *Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours*, 12(2) JIPLP 115 (2017).

[67] See ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW (Oxford University Press, 2015); Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in REINVENTING DATA PROTECTION (Serge Gutwirth et al. eds, 2009).

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

[69] *Id.*, at 63.

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

Some years later, in *Digital Rights Ireland*,[71] the Court invalidated Directive 2006/24/EC due to its disproportionate effects over fundamental rights,[72] by assessing, as a constitutional court, the interferences, and potential justifications, with the rights of privacy and data protection of EU citizens established by the Charter. The ECJ has shown itself to be aware of the risks of new technologies for 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."[73] Moreover, concerning automated technologies, the ECJ 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."[74]

The same constitutional approach can be appreciated in *Schrems*,[75] where the ECJ invalidated Decision 2000/520, which was the legal basis allowing the transfer of data from the EU to the US (i.e. safe harbor).[76] In this case, the interpretation of the ECJ 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."[77] Indeed, the ECJ manipulated the notion of "adequacy," which, as a result of this new constitutional frame, has moved to a standard of "equivalence" between legal orders.[78] Therefore, according to the ECJ, 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."[79]

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

[71] Cases C-293/12 e C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 2014 (decided Apr. 8, 2014). See, in particular, Federico Fabbrini, *The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS. J. 65 (2015).
[72] 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] OJ L 105/54.
[73] Digital Rights Ireland, *supra* note 71, at 56.
[74] *Id*, at 55.
[75] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015 (decided 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 GCYILJ 2016 245 (2017).
[76] 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] OJ L 215/7.
[77] Schrems, *supra* note 75, at 71.
[78] *Id*, at 73.
[79] *Id*.

perspective in the field of data is *Google Spain*, for at least two reasons.[80] Firstly, as in *Digital Rights Ireland* and *Schrems,* the Court granted a high level of protection to privacy and data protection to ensure the effective protection of these fundamental rights by virtue of a (constitutional) interpretation. Secondly, the *Google Spain* case demonstrates a first judicial attempt to face the power of online platforms and answer to the legislative inertia of the Union, thus, laying the foundation of digital constitutionalism.

The predominant role of Articles 7 and 8 can be observed by focusing on how the ECJ 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 ECJ 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."[81]

Secondly, the same consideration also applies to the definition of establishment. The ECJ 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.[82] As the ECJ observed, "[I]t 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."[83]

Thirdly, the ECJ has entrusted search engines to delist online content without removing information. Hence, the data subject has the right to request that the search engine obtain the erasure of the 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."[84] 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 ECJ 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 ECJ has delegated to search engines the task of balancing fundamental rights when assessing users' requests for the right to be forgotten.[85]

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 ECJ

[80] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 (decided May 13, 2014); Orla Lynskey, *Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez*, 78 MOD. L. REV. 522 (2015).
[81] *Id*., at 34.
[82] *Id.*, at 58.
[83] *Id.*, at 60.
[84] *Id.*, at 97.
[85] Jean-Marie Chenou & Roxana Radu, *The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union,* 58 B&S 74 (2017).

has been important to consolidate the constitutional dimension of privacy and data protection in the Union, the next subsection shows how the GDPR has tried to address the fallacies of EU data protection law, being one of the first expressions of digital constitutionalism.

4. The Third Season: Digital Constitutionalism

The turning of platforms' freedoms into new forms of power have led the Union to change its digital liberal approach and adopt a regulatory strategy. The roles and exploitation of new automated technologies for processing data by online platforms on a global scale have contributed, on the one hand, to introduce new ways and models to process vast amounts of content and data.[86] On the other hand, the implementation of these technologies has raised serious concerns regarding their degree of transparency and accountability,[87] requiring to rethink the protection of free speech and personal data in the information society.[88]

This scenario has not only challenged the protection of fundamental rights, such as freedom of expression and data protection by transnational corporations.[89] Even more importantly, the implementation of artificial intelligence technologies raises concerns for the democratic system and, especially, the principle of rule of law.[90] Technological evolutions, combined with a liberal constitutional approach, has led online platforms to autonomously set their rules and procedures. 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."[91] It is not by chance that these actors have been named "gatekeepers" to underline their high degree of control on online spaces.[92] Online platforms can autonomously decide not only how people interact but also how they can assert their rights (and what those rights are) by privately regulating their digital infrastructure.[93] In the lack of any regulation, these business choices play the role of the law in the digital environment on a global scale.

Therefore, 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). In particular, by implementing Terms of Service ("ToS"), platforms unilaterally establish what

---

[86] LUCIANO FLORIDI, THE FOURTH REVOLUTION HOW THE INFOSPHERE IS RESHAPING HUMAN REALITY (Oxford University Press, 2016).
[87] Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms* 3(1) BD&S (2016), https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512; Brent D. Mittlestadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BD&S (2016) https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679.
[88] 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).
[89] Gunther Teubner, *The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors*, 69(3) MOD. L. REV. 327 (2006).
[90] Paul Nemitz, *Constitutional Democracy and Technology in the age of Artificial Intelligence*, 2133 PHILOS. TRANS. ROYAL SOC. A (2018).
[91] Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, LAW AND POLITICAL ECONOMY (Dec. 6, 2017) https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon.
[92] Emily B Laidlaw, *A Framework for Identifying Internet Information Gatekeepers* 24(3) JIRLCT 263 (2012); Jonathan A Zittrain, *History of Online Gatekeeping* 19(2) HARV. J.L. & TECH. 253 (2006).
[93] 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 (Luca Belli and Nicolo Zingales eds, 2017)

users can do when accessing providers' services and how their data is processed, thus, exercising *de facto* tasks usually vested in public authorities.[94] By referring to Teubner, this framework could be described as "the constitutionalisation of a multiplicity of autonomous subsystems of world society."[95]

This situation also involves the relationship between online platforms and public actors. Governments and public administration usually rely on big tech companies, for instance, to offer new public services or improve their quality through digital and automated solutions.[96] However, this cooperation leads, firstly, tech companies to hold a vast amount of data coming from the public sector and, secondly, subject public actors to 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.[97] This relationship does not only affect principles such as transparency or fairness, but also, even more importantly, the principle of rule of law since legal norms are potentially replaced by technological or contractual standards established by transnational private actors.

Within this framework, the ECJ's judicial activism has played a crucial role in underling the new challenges of the information society, thus, triggering a new EU policy season (i.e. digital constitutionalism). As the expression suggests, digital constitutionalism is made of two main souls. The first term ("digital") refers to technologies based on the Internet like automated technologies to process data or moderate content. Whereas, the second word ("constitutionalism") refers to the political ideology born in the 18th century where, according to the Lockean idea, the power of governments should be legally limited and its legitimacy depends upon complying with these limitations.

Despite this chronological gap, the adjective "digital" entails the collocation of constitutionalism in a temporal and material dimension. Digital constitutionalism refers to a specific timeframe evolving in the aftermath 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 each other. Therefore, the merger of the expressions "digital" and "constitutionalism" does not lead to a new form of constitutionalism. Instead, it constitutes a new theoretical and practical field based on a dynamic dialectic between how digital technologies affects 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

---

[94] Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation*, 5(4) IPR (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?*, IRCLT (2018) https://www.tandfonline.com/doi/abs/10.1080/13600869. 2018.1475898.

[95] Gunther Teubner, *Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?*, in CONSTITUTIONALISM AND TRANSNATIONAL GOVERNANCE, (C. Joerges, I. Sand and G. Teubner eds, 2004).

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

[97] Sofia Ranchordas & Catalina Goanta, *The New City Regulators: Platform and Public Values in Smart and Sharing Cities*, CLSR (forthcoming 2019).

power ought to be limited (made legitimate) in the digital age."[98] Notwithstanding even the implementation of new digital technologies by public actors raises serious concerns, the rise of digital constitutionalism in the Union has been primarily driven by the role of transnational online platforms, which, although vested as private actors, increasingly perform quasi-public tasks.

Within the EU framework, the characteristics of this new constitutional season are based, firstly, on the codification of the ECJ's efforts to protect fundamental rights in the digital environment and, secondly, on the limitation on online platforms' powers by implementing legal instruments to increase the degree of transparency and accountability in online content moderation and data processing. Both of these characteristics can be found in the DSM strategy.[99] Online platforms should "protect core values" and increase "transparency and fairness for maintaining user trust and safeguarding innovation."[100] As the Commission underlined, the role of online platforms in the digital environment implies "wider responsibility."[101] Likewise, the Council of Europe has, on the one hand, underlined 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.[102] 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."[103]

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 process coming from legal institutionalization ("top-down") but from a social need ("bottom-up"). Like for other fields such as net neutrality or the right to Internet access, the introduction of new users' rights constitutes the expressions of key values of the contemporary society.[104] More specifically, the Directive on copyright in the DSM ("Copyright Directive"),[105] the proposal for regulation to tackle online terrorist content ("Regulation on Terrorist Content"),[106] and the adoption of the GDPR are just three of the examples demonstrating

[98] Nicolas Suzor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, 4(3) SM + S (2018), 4 https://journals.sagepub.com/doi/pdf/10.1177/2056305118787812.

[99] 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 [2015] COM(2015) 192 final.

[100] 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 [2016] COM(2016) 288 final.

[101] *Id.*

[102] Council of Europe, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, March 7, 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14, 6.

[103] *Id.*, at 7.

[104] Christoph B. Graber, *Bottom-Up Constitutionalism: The Case of Net Neutrality*, 7 TRANSNATIONAL LEGAL THEORY 524.

[105] 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.

[106] 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)).

how the EU approach aims to protect fundamental rights and limit the power of online platforms in the algorithmic society.

4.1 Content: Regulating Online Content Moderation

Within the framework of the DSM strategy, the Commission has launched legislative proposals to limit online platforms discretion and increase the degree of transparency and accountability in content moderation.[107]

The first example is the adoption of the Copyright Directive which, for the first time after almost twenty years, has introduced a new framework of liability for especially, online content-sharing service providers.[108] This step can be considered a watershed, acknowledging that the role of some online platforms (e.g. social media) cannot be considered merely passive any longer.

Since rightholders bear financial losses due to the quantity of copyright-protected works uploaded on online platforms without prior authorization, the Copyright Directive establishes, *inter alia*, a licensing system between online platforms and rightsholders.[109] More specifically, 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, of copyright-protected works unless they comply with the new exception of liability.[110]

The heritage of the ECJ rulings in terms of proportionality safeguards is evident. Indeed, 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."[111] Moreover, this regime partially applies to online content-sharing service providers whose services have been available to the public in the Union for less than three years and that have an annual turnover below €10 million.[112] Furthermore, the cooperation between rightsholders and online platforms should not lead to any general monitoring obligations pursuant to the decisions of the ECJ in *Scarlet* and *Netlog*.[113]

This new system of liability is not the sole novelty. Indeed, the Union has not only codified the findings of the ECJ but has reached another turning point in its (digital) constitutional approach by limiting online platforms' powers by introducing due process safeguards through obligations of transparency and accountability in content moderation. For instance, online

[107] Giovanni De Gregorio, *Expressions on Platforms: Freedom of Expression and ISP liability in the Digital Single Market*, 3(2) CoRe 213 (2018).
[108] Martin Husovec, *How Europe Wants to Redefine Global Online Copyright Enforcement*, in Pluralism or Universalism in International Copyright Law (Tatiana E. Synodinou ed., forthcoming 2019); Giancarlo Frosio & Sunimal Mendis, *Monitoring and Filtering: European Reform or Global Trend?*, in The Oxford Handbook of Online Intermediary Liability (Giancarlo Frosio ed., forthcoming 2019).
[109] *Id.*, art. 2(6).
[110] *Id.*, art. 17.
[111] *Id.*, art. 17(5).
[112] *Id.*, art. 17(6).
[113] *Id.*, art. 17(8).

content-sharing service providers are required to implement an effective and expeditious complaint and redress mechanism that is available to the users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject-matter uploaded by users.[114] 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.

Similar observations apply to the proposal for a Regulation on Terrorist Content which aims to establish a clear and harmonized legal framework to prevent the misuse of hosting services for the dissemination of this type of content.[115] Firstly, the proposal defines terrorist content.[116] As a result, since the definition is provided by law, online platforms discretion would be bound by this legal definition when moderating terrorist content. Secondly, 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.[117]

Despite the relevance of these obligations, the implementation of these measures, described as "duties of care,"[118] should not lead online platforms to generally monitor the information they transmit or store, nor to a general duty to actively seek 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 remove expeditiously the content of which they became aware. Besides, online platforms are obliged to remove content within one hour of the receipt of a removal order from the competent authority.[119]

Even in this case, the Union has tried to inject procedural safeguards requiring, for example, to set out clearly in their terms and conditions their policy to prevent the dissemination of terrorist content.[120] As a general rule, online platforms should protect their services against the public dissemination of terrorist content but 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."[121] Transparency obligations are not the only safeguards. Indeed, where hosting service providers use automated tools in respect of content that 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).[122] Furthermore, it recognizes the right to an effective remedy requiring online

[114] *Id.*, art. 17(9).
[115] 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 (2019), https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf; Joan Barata, *New EU Proposal on the Prevention of Terrorist Content Online*, CIS Stanford Law (2018) https://cyberlaw.stanford.edu/files/publication/files/2018.10.11.Comment.Terrorism.pdf.
[116] Regulation on terrorist content, art. 2(1)(5).
[117] *Id.*, art. 3.
[118] *Id.*
[119] *Id.*, art. 4(3).
[120] *Id.*, art. 8(1).
[121] *Id.*, art. 6.
[122] *Id.*, art. 9(2).

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.[123]

These two examples show how the Union has, on the one hand, codified the lessons of the ECJ 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 examine the EU approach to online platforms just from a hard law perspective. Indeed, the Commission has introduced codes of conducts and guidelines to nudge online platforms to introduce transparency and accountability mechanisms.[124] In particular, the Recommendation on measures to effectively tackle illegal content online propose a general framework of safeguards in content moderation.[125] 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.[126] 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.[127] Against a removal decision, the content provider should have the possibility to contest the decision by submitting a "counter-notice" within a "reasonable period of time." The Recommendation in question can be considered the 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 automated technologies.

Despite the step forward made in the last years at EU level, this supranational approach has not preempted Member States in following their path in the field of content moderation, especially when looking at the law introduced by Germany in the field of hate speech,[128] and France concerning disinformation.[129] Taking as an example the German case, in 2017, the German Network Enforcement Act requires social media receiving more than 100 reports of illegal content in a calendar year to submit a six-monthly report on their content moderation activities.[130] Even more importantly, this German law introduces a procedure to manage complaints regarding illegal content.[131] Among the obligations, social media have to remove or block access to content that is

[123] *Id.*, arts 9(a)-11.
[124] Code of conduct on countering illegal hate speech online, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300; Code of practice on disinformation, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation; 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.
[125] Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C (18) 1177 final.
[126] *Id.*, at 16.
[127] *Id.*, at 9.
[128] Netzdurchsetzunggesetz, Law of 30 June 2017 ("NetzDG").
[129] Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information; Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
[130] 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 (Bilyana Petkova & Tuomas Ojanen eds, 2019).
[131] NetzDG, *supra* note 128, art. 3.

manifestly unlawful within 24 hours of receiving the complaint. Outside this case, social media are required to remove or block a specific content being within seven days of receiving the complaint with some exceptions.[132] Failure to comply with the provisions of this law can lead to fines up to fifty million euros.[133]

Although the EU legal framework has made some important step forward in the field of content moderation, however, the legal fragmentation of guarantees and remedies at supranational and domestic level could undermine the attempt of the Union to provide a common framework to address the cross-border challenges raised by online platforms in the field of content. In other words, if the "power of positive thinking" has led the Union to introduce significant transparency and accountability safeguards,[134] the mix of supranational and national initiatives leads to decrease the effective degree of protection for individuals and undermining fundamental freedoms and rights in the internal market, thus, challenging the role of digital constitutionalism in protecting individuals fundamental rights and limiting the powers of online platforms.

4.2 Data: The General Data Protection Regulation

The constitutional path of the protection of personal data has reached a new step, not only in the aftermath of Lisbon thanks to the role of the ECJ but also with the adoption of the GDPR. The expression of the new digital constitutional approach of the Union is clear when comparing the first Recitals of the GDPR with the Data Protection Directive to understand the central role of data subjects' fundamental rights within the framework of EU data protection law,[135] as also resulting from the case law of the ECJ in the field of digital privacy.

In order to achieve this objective without neglecting the need to protect other constitutional interests clashing the right to privacy and data protection,[136] the entire structure of the GDPR is based on general principles which orbit around the accountability of the data controller, who should ensure and prove compliance with the general principles.[137] Even when the data controller is not established in the Union according to some conditions,[138] 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 the risk for data subjects.[139] In other words, even in this field, the approach of the Union aims to move from formal compliance as legal shields to substantive responsibilities (or accountability) of the data controller whose beacon are 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

[132] *Id.*, art. 1(3).
[133] *Id.*, art. 4.
[134] Aleksandra Kuczerawy, *The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*, in 8 JIPITEC 226 (2017).
[135] GDPR, *supra* note 45, Recitals 1-2.
[136] *Id.*, Recital 4.
[137] *Id*, art. 5.
[138] *Id.*, art. 3(2).
[139] Claudia Quelle, *The Risk Revolution in EU Data Protection Law: We Can't Have our Cake and Eat it, Too*, in DATA PROTECTION AND PRIVACY: THE AGE OF INTELLIGENT MACHINES (Ronald Leenes et al. eds, 2017).

the purposes of the processing, as well as the risks to the individuals' rights and freedoms. 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.[140]

The principles of privacy by design and by default contributes to achieving this purpose by imposing an ex-ante assessment of compliance with the GDPR and, as a result, with the protection of the fundamental right to data protection.[141] Put another way, the GDPR focuses on promoting a proactive, rather than a reactive approach based on the assessment of the risks and context of specific processing of personal data. A paradigmatic example of this shift is the obligation for the data controller to carry out the Data Protection Impact Assessment, which explicitly also aims to 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."[142] This obligation requires the data controllers to conduct a risk assessment which is not only based on business interests but also on data subjects (fundamental) rights.

Furthermore, the GDPR has not only tried to increase the degree of accountability of the data controller but also empowered individuals by introducing new data subjects' rights demonstrating how the Union intends to ensure that individuals are not marginalized vis-à-vis the data controller, especially, when the latter process vast amounts of data and information through the use of artificial intelligence technologies. Among these safeguards, it is not by chance that the GDPR establishes the right not to be subject to automated decision-making processes as an example of the Union reaction against the challenges raised by artificial intelligence technologies. Without being exhaustive, Article 22 provides a general rule, according to which, subject to some exceptions,[143] the data subject has 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."[144] This provision has been interpreted more as a liberty or a general prohibition, rather than a right of the data subject.[145] Therefore, the data subject does not need to express any positive conduct to rely on this right, thus, requiring the data controller to avoid interference with this right like 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, express his or her point of view and contest decisions.[146] 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"

[140] *Id.*, art. 24.
[141] *Id.*, art. 25.
[142] *Id.*, art. 35(3)(a).
[143] *Id.*, art. 22(2).
[144] Sandra Watcher & Brendt Mittlestadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, COLUM. BUS. L. REV. 494 (2019).
[145] Working Party 29, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (February 6, 2018).
[146] GDPR, *supra* note 45, art. 22(3).

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 triggered a debate among scholars on whether the GDPR provides effective grounds to protect from potentially harmful consequences coming from automated decision-making processes, most notably by creating a "right to explanation." [147] Some of them argue that the GDPR fosters qualified transparency over algorithmic decision-making.[148] Instead, others support or question the existence of such a right,[149] or doubt that the GDPR offers a concrete remedy to algorithmic decision-making processes.[150] What is true is that this data subject's right does not solve the new challenges raised by the algorithmic society. Firstly, 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. Secondly, the presence of a human being does not eliminate any risk of error or discrimination. Thirdly, 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.[151] From a constitutional perspective, Article 22 provides a safeguard against the massive spread of artificial intelligence technologies promising to replace man in decision-making activities and increasingly affecting individuals' rights. Indeed, 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 control. This situation raises threats not only for the principles of EU 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 clear answer to these challenges and, more in general, to the fallacies of EU data protection law.[152] 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 enough to protect the fundamental rights of data subjects in a specific context. In other words, the risk-based approach introduced by the

---

[147] See, in particular, Bryce Goodman & Set Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation",* 38 AI MAGAZINE 50 (2017); Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7(4) IDPL 233 (2017).

[148] Margot E. Kaminski, *The Right to Explanation, Explained*, 34(1) BERKELEY TECH. L.J. (2019).

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

[150] 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).

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

[152] Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 IDPL 250 (2014).

GDPR could be considered a delegation to data controller of the power to balance conflicting interests, thus, making the controller the "arbiter" of data protection. Although the GDPR cannot still be considered the panacea of digital constitutionalism, however, it constitutes an important step forward in the field of data. Like in the case of content, the Union approach has focused its efforts on limiting discretion in the use of algorithmic technologies and empowering data subjects with new rights in the algorithmic society in light of the constitutional protection ensured by Articles 7 and 8 of the Charter.

5. Toward a Fourth Phase of the EU Policy in a Global Context?

The analysis of the fields of content and data provides clues to understand the reasons for this new constitutional moment, showing why the Union has changed its policy by complementing its liberal goals with a new (digital) constitutional strategy.

The liberal narrative characterizing the Union's policy at the beginning of this century has slowly faded away. Indeed, if, on the one hand, promoting the development of digital services has played a crucial role for the development of the internal market, on the other hand, a liberal approach in this field has also contributed to challenging users' fundamental rights and allowing the growth of new private founding powers. The phase of judicial activism has been the first reaction against this situation and, also, one of the most important steps towards digital constitutionalism. In order to answer to a phase of legislative inertia, the ECJ has underlined 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 season of EU (digital) constitutionalism. The codification of the ECJ efforts and the regulation of online platforms' activities have been the answers characterizing the third phase of EU policy opposing the troubling rise and evolution of private powers in the algorithmic society.

Despite the aforementioned challenges, the Union has not introduced censoring provisions to online content or prohibiting the use of some technologies to process data. On the opposite, the EU strategy has been based on introducing safeguards to foster transparency and accountability in online content moderation and data processing. This new phase of EU constitutionalism has not led to a dangerous escalation of authoritarian answers but to regulatory solutions aimed to protect of fundamental rights in a societal environment which strongly differs from the framework at the end of the last century. The possibility for individuals to, for example, obtain justification for automated outcomes, access redress mechanisms, or human intervention would mitigate the gap between humans and machines.[153] Stated differently, these new rights would allow users to rely on a (first) "human translation" of the algorithmic process. As Pasquale explained, "without 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."[154]

[153] 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).

[154] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 9 (Harvard University Press, 2015).

Within this scenario, the rise of digital constitutionalism represents the end of the Union liberal approach and a potential basis for promoting an EU democratic digital environment. However, digital constitutionalism looks far from being the last step of the EU regulatory path. At this time, it would be already possible to frame a new evolving trend of the EU policy characterized by the extension of constitutional values beyond EU borders and the expression of a human-centric technological model.

In the field of content, the provisions established by the Copyright Directive and the Regulation on Terrorist Content would require transnational corporations to comply with new obligations concerning content moderation.[155] In particular, this approach could provide global benefit since online platforms would be encouraged to set the degree of protection required by EU law as a general standard on a global scale to avoid the financial and organizational burden coming from the adoption of different models of content moderation. The ECJ's decision in *Glawischnig-Piesczek* contributes to outline this scenario.[156] In this case, where the applicant sought a judicial order requiring Facebook to cease publication of "identical" or "equivalent content" on a global scale, the ECJ recognized that the e-Commerce Directive does not preclude the global scope of the measures which Member States are entitled to adopt.[157] Indeed, according to the ECJ, "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."[158] As a result, the ECJ ruled that the EU law allows to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law, and it is up to Member States to take that law into account.[159]

In the field of data, the potential extension of EU constitutional values is even more evident.[160] If, in *Schrems*, the ECJ has already shown the ability of EU 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 GDPR's scope of application has codified several judicial attempts by the ECJ to ensure the effective protection of the rights of EU citizens beyond its borders.[161] In particular, the GDPR does not only state that EU 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."[162] Indeed, it completes this framework by establishing that, even though the controller is established outside the Union, the GDPR is nevertheless applicable if the activities that the processing of personal data consists of the

[155] The Regulation on Terrorist Content clarifies that its scope of application extends to "hosting service providers offering services in the Union to the public, irrespective of their place of main establishment." Regulation on Terrorist Content, *supra* note 106, Art 1(2).
[156] Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, 2019 (dec. Oct. 3, 2019).
[157] *Id.*, at 49-50.
[158] *Id.*, at 51.
[159] Lorna Woods, *Facebook's Liability for Defamatory Posts: The CJEU Interprets the E-commerce Directive*, EU LAW ANALYSIS (Oct. 7, 2019) http://eulawanalysis.blogspot.com/2019/10/facebooks-liability-for-defamatory.html.
[160] Christoper Kuner, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, 5 IDPL 23 (2015).
[161] C-131/12, *supra* note 80; Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 2015 (dec. Oct., 1 2015).
[162] GDPR, *supra* note 45, art 3(1).

provision of products or services to individuals residing in the Union or the targeting of consumers' behavior.[163] This provision can be considered the result of the high-level constitutional standard of protection in the EU, which, in the information society, cannot be limited to the EU territory any longer "in order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation."[164]

The consequence of such a rule is twofold. On the one hand, this provision involves jurisdiction. The GDPR's territorial scope of application overcomes the doctrine of establishment developed by ECJ 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,[165] the "global reach of EU law",[166] or, more in general, the "Brussel effect" to describe the power of the Union to export its policy on a global scale.[167]

Nevertheless, the extension of data protection rules to the global context could also lead to some drawbacks. Indeed, the scope of application extending beyond EU borders could also 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, "when 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."[168]

Furthermore, the outreaching scope of EU constitutional values could affect the right to freedom of expression and financial interests of other countries and their citizens.[169] The ECJ has recently highlighted this challenges in the decision *Google v. CNIL* where the core of the preliminary questions raised by the French judge aimed to clarify the boundaries of the right to be forgotten online, especially its global scope.[170] According to the ECJ, on the one hand, search engines organize information contained in a list of results displayed following a search conducted on the basis of an individual's name ubiquitous, 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."[171] However, on the other hand, the right to the protection of

[163] *Id.*, art. 3(2).
[164] *Id.*, Recital 23.
[165] 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 IDPL 28 (2018).
[166] Christopher Kuner, *The Internet and the Global Reach of EU Law*, EU LAW BEYOND EU BORDERS: THE EXTRATERRITORIAL REACH OF EU LAW (Marise Cremona and Joanne Scott eds, 2019).
[167] Anu Bradford, *The Brussel Effect*, 107 NW. U. L. REV. (2015). See also the position of Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 AJCL 87 (2014).
[168] 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 IDPL 230 (2016), 240
[169] Dan J.B. Svantesson, *A "Layered Approach" to the Extraterritoriality of Data Privacy Laws*, 3 IDPL 278 (2013), 1
[170] Case C-507/17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), (2019) (dec. Sept. 24, 2019).
[171] *Id.*, at 58.

personal data is not an absolute right, but be balanced with other fundamental rights in relation to its function in society and in accordance with the principle of proportionality.[172] Therefore a global delisting would interfere with freedom of expression on a global scale leading to extend EU constitutional values also to third States which do not recognize the right to delisting.

This trend seems to suggest how the Union approach does not aim to extend its law over its territorial boundaries but to avoid that online platforms formally rely on their geographical location (*rectius*, establishment) as a shield to avoid compliance with EU law. If, on the one hand, the Union would aim 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 fourth phase of EU policy could be triggered by the need to protect fundamental rights in a global context where other countries are still following a (digital) liberal approach like the US, at least at federal level, or playing a predominant role in the rush for the primacy over artificial intelligence technologies like China. In other words, rather than a "European data privacy imperialism," [173] the fourth phase of the EU policy would lead to a new phase of transnational constitutional law aimed to protect individuals' fundamental rights in the algorithmic society. It is not by chance that, recently, the High-Level Expert Group on Artificial Intelligence proposed a human-centric approach for all automated systems.[174] Not a long time ago, 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."[175]

These statements should not surprise but underline one of the essential peculiarities of EU constitutionalism whose roots are based on human dignity.[176] Against the threats coming from ubiquitous automation putting aside people out of the equation as far as possible, the Union approach can rely on a constitutional humus able to tackle potential trend which would replace human beings with automated technologies. While digital constitutionalism has shown the talent of constitutional law to react against the threats to fundamental rights raised by the exercise of "private powers" in the digital environment, a fourth phase, or better a more sophisticated expression of digital constitutionalism called digital humanism, would be the basis to address the new threats to individuals' dignity. In other words, the fourth phase of the digital constitutionalism should not be seen just as the imperial extension of legal provisions outside the territory of the Union but as the reaction of European constitutionalism against the challenges for human dignity coming from new technologies in the algorithmic society. In this scenario, the evolution of digital constitutionalism would oppose to techno-determinist solutions and contribute to promoting EU

[172] *Id.*, at 60. See, also, Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen. (dec. Nov. 9, 2010), at 48; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, at 136.
[173] Svantesson, *supra* note 169, 279.
[174] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, April 8, 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.
[175] European Data Protection Supervisor, *Opinion 4/2015, Towards a New Digital Ethics*, September 11, 2015, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_ en.pdf.
[176] CATHERINE DUPRÈ, THE AGE OF DIGNITY HUMAN RIGHTS AND CONSTITUTIONALISM IN EUROPE (Hart, 2016).

values as a sustainable constitutional model for the development of automated technologies on a global context.