SCUOLA DI DOTTORATO
UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA

Department of Law

PhD program in Legal Studies Cycle XXXIII

Curriculum in Public Law

CONSTITUTIONAL LAW IN THE INFORMATION SOCIETY: PROTECTING FUNDAMENTAL RIGHTS AND DEMOCRACY IN THE AGE OF ARTIFICIAL INTELLIGENCE

De Gregorio Giovanni

835505

Tutor: Prof. Giulio Enea Vigevani

Coordinator: Prof. Stefania Ninatti

ANNO ACCADEMICO / ACADEMIC YEAR 2019/2020

Table of Content

Chapter I

Introduction

Summary: 1. Constitutionalising Global Private Spheres. – 2. Content and Data in the Algorithmic Society. – 3. Reframing Constitutional Law in the Information Society. – 4. The Forgotten Talent of European Constitutional Law. – 5. Investigating European Digital Constitutionalism. – 6. Research Structure.

1. Constitutionalising Global Private Spheres

The spread of digital technologies has led to disruptive effects on the society of this century.[1] The daily life is going digital towards an 'onlife' dimension.[2] Individuals increasingly experience their rights and freedom in a ubiquitous digital environment shaped by a mix of entities expressing forms of public authority and private ordering.[3] The pandemic season has been a litmus test showing how transnational private actors are critical infrastructures of the information society.[4] In this context, social subsystems like law, technology and society produce their internal norms while continuously shaping each other in a process of mutual influence or rather digital constitutivity. The law is the result of the compromise between technological architecture, social norms and market forces competing online.[5] At the same time, the law, as a social subsystem, indirectly influences the other environments.[6] Usually, recognised powers derive from legal categories such as rules, authority or rights and freedoms. These definitions do not exist outside the legal framework but are created by the law. The influence of legal systems through legal definitions, scope and enforcement of regulation shape the boundaries and characteristics of technology and society.[7] In other words, the peculiarity of the law as a social subsystem is to define spaces representing delegated and autonomous manifestations of powers.

Within this framework, constitutional law was not spared. The path towards the shift from atoms to bits started at the end of the last century has affected constitutional values like the protection of fundamental rights and democracy,[8] ultimately, leading to a new digital

[1] Sherry Turkle, 'How Computers Change the Way We Think' (2004) 50 The Chronicle of Higher Education B26.
[2] Luciano Floridi (eds), *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Springer 2015).
[3] Julie E. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (Oxford University Press 2020).
[4] Nikolas Guggenberger, 'Essential Platforms' SSRN (7 October 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3703361> accessed 16 October 2020; Jennifer Cobbe and Elettra Bietti, 'Rethinking Digital Platforms for the Post-COVID-19 Era' CIGI (12 May 2020) <https://www.cigionline.org/articles/rethinking-digital-platforms-post-covid-19-era> accessed 3 July 2020.
[5] Lawrence Lessig, *Code: And Other Laws of Cyberspace. Version 2.0* (Basic Books 2006).
[6] Gunther Teubner, *Law as an Autopoietic System* (Blackwell 1993).
[7] For instance, the notion of 'space' (and 'cyberspace') are legally constituted and shaped over time. David Delaney, 'Legal Geography I: Constitutivities, Complexities, and Contingencies' (2015) 39(1) Progress in Human Geographies 96.
[8] Oreste Pollicino and Graziella Romeo (eds), *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe* (Routledge 2016); Tommaso E. Frosini,

constitutional phase at the door of the algorithmic society.[9] In the aftermath of the Internet, digital technologies have triggered the development of new channels, products and services, extending the opportunities to exercise economic freedoms and fundamental rights like freedom of expression or the freedom to conduct business. The Internet has fostered the possibilities to share opinions and engage with other people, thus, fostering civil and political rights. The digital environment also provided opportunities to foster the protection of other constitutional interests like association.[10] This was also one of the primary reasons justifying the technological optimism at end of the last century which considered the digital environment as an opportunity to increase users' empowerment while limiting public interference.[11]

From a constitutional standpoint, this new Copernican revolution has led to a positive alteration of the constitutional stability. The ubiquity of digital technologies and the role of online platforms have affected how content and data are produced and processed online by implementing algorithmic technologies. Content and data can easily be disseminated on a global scale to access services provided for free like e-mail services or social media platforms. At first glance, the benefits of this revolution of freedom would overcome any drawback, especially when thinking about public surveillance and monitoring. Nonetheless, the digital environment is far from being outside forms of control. Apart from the interferences of public actors,[12] the digital environment is indeed subject to the authorities (or governance) of private actors designing the digital world we are experiencing in our daily lives. Google, Facebook, Amazon and Apple are paradigmatic examples of new digital forces competing with public authorities in the exercise of powers online.

In the information society, we are witnesses of a process guided by new entities which are neither public actors nor entities representing the will of the people, but still establishing standards of protection on a global scale beyond the democratic sovereign will. We are experiencing constitutional changes which are not the result of democratic processes, but the power of private actors to push lawmakers and courts to adapt legal norms to the challenges of the information society. We cannot define this as a democratic constitutional moment in Ackerman's terms.[13] The rise and consolidation of private powers online lead us before something different. Ackerman theory looks at constitutional values not just as a mix of expressions and courts' interpretations, but the set of principles agreed by the people in extraordinary moment of constitutional participation. Instead, the rise of transnational private actors imposing their governance online

---

'Internet come ordinamento giuridico' (2014) (1) Percorsi costituzionali 13; G. De Minico, *Internet. Regola e anarchia* (Jovene 2012); Vittorio Frosini, 'L'orizzonte giuridico dell'internet' (2000) (2) Diritto dell'Informazione e dell'informatica 270; Pasquale Costanzo, 'Aspetti evolutivi del regime giuridico di Internet' (1996) (6) Diritto dell'Informazione e dell'informatica 831.

[9] Paul Nemitz, 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) Royal Society Philosophical Transactions A 376.

[10] Silvia Sassi, 'La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della Costituzione. Il (recente) caso dell'associazione xenofoba' in AA. VV., *Da Internet ai Social Network* (Maggioli 2013) 33: Massimiliano Mezzanotte, 'Nuovi media e liberta antiche: la liberta di associazione in Internet' in Tommaso E. Frosini and others (eds), *Diritti e libertà in Internet* 231 (Le Monnier 2015).

[11] David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1371.

[12] Justin Clark and others, 'The Shifting Landscape of Global Internet Censorship' (2017) Berkman Klein Center for Internet & Society Research Publication <https://dash.harvard.edu/handle/1/33084425> accessed 4 February 2020.

[13] Bruce Ackerman, *We The People: Transformations* (Belknap Press 1998).

represents the constitutionalisation of global private spheres. In this process, constitutional values as interpreted by courts and implemented by lawmakers respectively when taking decisions and enacting legislation are under a process of amendment and redefinition which it is not expressed by codification but a contamination of private determinations. This is a clear example of how the internal rules produced by social subsystems compete with the autopoietic characteristics of (constitutional) law. By referring to Teubner, this framework could be described as 'the constitutionalisation of a multiplicity of autonomous subsystems of world society'.[14]

The constitutionalisation of global private spheres in the information society should not be seen only as an isolated phenomenon but it is a piece of the puzzle in the process of globalisation where new technologies have challenged the traditional Westphalian principle of sovereignty and territory.[15] From a transnational constitutional perspective, one of the primary concerns of democratic constitutional states when dealing with transnational phenomena occurring outside their territory.[16] However, even constitutional law is changing. Local dynamics and values still constitute the basic roots of each constitutional system. Still, supranational and international bundles, as in the case of the consolidation of multilevel constitutionalism in the European experience,[17] leads to the emancipation of constitutional law from local towards a more global character where constitutional systems increasingly meet in a process of global hybridisation. In the last thirty years, globalisation has affected legal systems,[18] thus, causing a constitutional distress.[19] Traditional legal categories have been put under pressure.[20] We have experienced the rise of different institutions at the global level whose rules extend their scope on a global scale.[21] Financial markets or environmental standards are paradigmatic examples of sectors where political choices are increasingly taken outside traditional democratic circuits. Powers are also exercised by private groups adopting rules governing society.[22]

Together with these transnational phenomena, the Internet has played a pivotal role in the rise of new private powers.[23] This new protocol of communication has provided new opportunities to

[14] Gunther Teubner, 'Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?' in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism* 3 (Hart 2004).
[15] Oreste Pollicino and Marco Bassini, 'The Law of the Internet between Globalisation and Localization' in Miguel Maduro, Kaarlo Tuori and Suvi Sankari (eds), *Transnational Law. Rethinking European Law and Legal Thinking* 346 (Cambridge University Press 2016).
[16] Eric C Ip, 'Globalization and the Future of the Law of the Sovereign State' (2010) 8(3) International Journal of Constitutional Law 636.
[17] Ingor Pernice, 'Multilevel Constitutionalism and the Crisis of Democracy in Europe' (2015) 11(3) European Constitutional Law Review 541.
[18] Francesco Galgano, *La globalizzazione nello specchio del diritto* (Il Mulino 2005).
[19] Mark Tushnet, 'The Inevitable Globalization of Constitutional Law' (2009) 49 Virginia Journal of International Law 985.
[20] Andrea Simoncini, 'Sovranità e potere nell'era digitale', in Tommaso E. Frosini and others (n 10), 19.
[21] Maria Rosaria Ferrarese, *Le istituzioni della globalizzazione. Diritto e diritti nella societa' transnazionale* (Il Mulino 2000).
[22] Louis L. Jaffe, 'Law Making by Private Groups' (1937) 51(2) Harvard Law Review 201.
[23] Pietro Sirena and Andrea Zoppini (eds), *I poteri privati e il diritto della regolazione* (Roma TrE-Press 2018); Francesco Mezzanotte, 'I poteri privati nell'odierno diritto dello sviluppo economico' (2018) (3) Politica del diritto 507; Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016); Cesare M. Bianca, *Le autorita private* (Jovene 1977); Giorgio Lombardi, *Potere privato e diritti fondamentali* (Giappichelli 1970).

exercise fundamental rights and freedoms.[24] At the same time, it has led to wondered about the relationship between liberty and power in the information society.[25] The rise of private institutions online which increasingly mirror traditional public powers questions how constitutional law traditionally protects fundamental rights and democratic values.

2. Content and Data in the Algorithmic Society

The fields of online content and data can provide interesting clues to explain this change of paradigm in the exercise of power. In terms of speech, the digital environment has become a primary channel for individuals to exercise their rights and freedoms, especially freedom of expression.[26] The Internet and related services have fostered the dissemination of information increasing the opportunities of each individual to share ideas and opinion on a global scale without supporting the infrastructural costs and content filters of traditional media outlets. The early days of the digital environment had promised a positive evolution of the public sphere and democracy through the citizens' empowerment coming from decentralisation and anonymity. This positive trend was confirmed in a countless number of cases. It would be enough to mention how social media and search engines have provided irreplaceable tools for exercising speech rights like the right to inform and be informed. Online speech has shown its ability to influence elections, rise the exchange of new ideas on a global scale as well as supporting minorities and political movements as an instrument of emancipation like the Arab Spring.[27]

While, at first glance, individuals would access more possibilities to share their ideas and opinions online, however, a closer look reveals that the flow of information online is not without control. Somewhat, in the last years, States, especially authoritarian and totalitarian countries, have censored speech by shutting down the Internet extensively despite the economic consequences.[28] Even democratic countries have extended their regulation over extreme content (e.g. hate speech) or tackle the spread of unauthorised copyright content. Still, unlike authoritarian countries, constitutional democracies have shown a more neutral approach without falling in emotionalism or extensive censoring mechanisms. The constitutional boundaries which require constitutional democracies not to disproportionately interfering with fundamental rights, primarily, in this case, freedom of expressions, have constituted critical safeguards to mitigate the potential escalation of shutdowns and general censorship.

Nonetheless, this situation is not merely related to online censorship by public authorities which are already subject to constitutional obligations. In democratic countries, the concerns about the flow of information online do not just regard the role of public authorities but also

[24] Jack M. Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 New York University Law Review 1.
[25] Stefano Rodotà, *Foucault e le nuove forme del potere* (La Biblioteca di Repubblica 2011); Vittorio Frosini, *Il diritto tra potere e libertà nell'era tecnologica*, in Vittorio Frosini, *Il giurista e le tecnologie dell'informazione* (Bulzoni Editore 1998), 37; James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' (1997) 66 University of Cincinnati Law Review 177.
[26] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006).
[27] Gadi Wolfsfeld and others, 'Social Media and the Arab Spring: Politics Comes First' (2013) 18(2) The International Journal of Press/Politics 115.
[28] Giovanni De Gregorio and Nicole Stremlau, 'Internet Shutdowns and the Limits of Law' (2020) 14 International Journal of Communication 4224.

private actors, precisely online platforms in exercising powers over speech.[29] By implementing artificial intelligence systems, platforms, like Facebook or YouTube, can decide how to display and organise content based on opaque criteria and their business purposes, thus, influencing public discourse. Therefore, individuals interact with information and products online which resemble their interests and preferences with pervasive effects on self-determination and media pluralism. It is not by chance that Pariser and Sunstein have underlined the risk of polarisation due to the creation of 'filter bubbles' or 'information cocoons'.[30] Although the Internet has enhanced the abilities of individuals to access different types of information, this positive effect is lessened by a substantial restriction in the autonomy of users subject to what Cohen defines as a 'modulated democracy'.[31] From a constitutional point of view, the primary concern in democratic countries comes from the traditional vertical nature characterising the protection of the right to freedom of expression. Unlike public actors, online platforms are not required to ensure the same constitutional safeguards when they take decisions over the organisation or removal of speech online. These actors can enforce and balance the vast amount of speech online outside any public safeguard like the rule of law.

Likewise, even in the field of data, it is possible to observe the critical role of online platforms in the information society. At the end of the last century, the digital environment was considered a space to ensure the protection of privacy through anonymity and decentralisation. It is not by chance whether one of the most famous slogans was 'On the Internet, nobody knows you are a dog'.[32] As observed by Turckle, '[y]ou can be whoever you want to be. You can completely redefine yourself if you want. You don't have to worry about the slots other people put you in as much. They don't look at your body and make assumptions. They don't hear your accent and make assumptions. All they see are your words'.[33] The fact is that words are also data which can be processed for extracting values and predictive answers. This deals with the issue of anonymity at the intersection between freedom of expression and privacy.[34] The relevance of data in the

[29] Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 U.C. Davis Law Review 1151; James Grimmelmann, 'Speech Engines' (2014) 98 Michigan Law Review 868; Stuart Minor Benjamin, 'Algorithms and Speech' (2013) 161(4) University of Pennsylvania Law Review 1446.

[30] Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (Viking 2011); Cass R. Sunstein, *Republic.com 2.0* (Princeton University Press 2007).

[31] Julie E. Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904.

[32] This is an adage by Peter Steiner and published by The New Yorker in 1993. Glenn Fleishmandec, 'Cartoon Captures Spirit of the Internet' The New York Times (14 December 2000) <https://www.nytimes.com/ 2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> accessed 29 January 2020.

[33] Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster Trade 1995), 184-185.

[34] Giorgio Resta, 'L'anonimato in Internet', in Tommaso E. Frosini (n 10); Marco Betzu, 'Anonimato e responsabilità in internet' (2016) costituzionalismo.it <https://www.costituzionalismo.it/anonimato-e-responsabilita-in-internet/> accessed 6 October 2020; Giulio E. Vigevani, 'Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano' (2014) (2) Diritto dell'informazione e dell'informatica 207; Giorgio Resta, 'Anonimato, responsabilità, identificazione: prospettive di diritto comparato' (2014) (2) Diritto dell'informazione e dell'informatica 171; Vincenzo Zeno-Zencovich, 'Anonymous speech on the Internet' in Andras Koltay (ed), *Media Freedom and Regulation in the New Media World* 103 (Wolters Kluwer 2014); Michela Manetti, 'Liberta di pensiero e anonimato in rete' (2014) (1) Diritto dell'informazione e dell'informatica 139; Marco Cuniberti, 'Democrazie, dissenso politico e tutela dell'anonimato' (2014) (2) Diritto dell'informazione e dell'informatica 111; Giovanni M. Riccio, 'Anonimato e responsabilità in Internet' (2000) (2) Diritto dell'informazione e dell'informatica 314; Enrico

information society has already highlighted serious constitutional challenges at the beginning of this century,[35] especially with the evolution of profiling technologies.[36] As observed by Nissenbaum, 'in a flourishing online ecology, where individuals, communities, institutions, and corporations generate content, experiences, interactions, and services, the supreme currency is information, including information about people'.[37] The development and implementation of algorithmic technologies have increased the concerns for the protection of privacy and personal data subject to ubiquitous forms of control answering to the logic of accumulation, prediction and behavioural influences.[38] The Cambridge Analytica scandal showed that platforms play a critical role not only in the processing of data but also affects democracy.[39] In a circular way, it has been the role of new technologies to trigger the emergence of data protection as a new and autonomous fundamental right in the European framework,[40] and it is still technology challenging the protection of individuals' privacy.

At the end of the last century, the development of new processing technologies has allowed the rise of new business models based on the processing of multiple kind information including personal data which are increasingly collected, organised and processed both by public actors for pursuing public tasks and business actors for profits. Put another way, like in the field of expressions, the value of data in the algorithmic society can be understood by focusing on artificial intelligence systems providing new opportunities for businesses from the processing of (personal) data. The extraction of value by automated processing is a paradigmatic example.[41] Even in this case, online platforms play a critical role due to the vast amount of data they process and organise. Even if not exclusively, their business model is based or highly rely on the processing of data for profiling purposes to make profits from advertising revenues, targeted services or analysis of data.

Since data and information constitute the new non-rival and non-fungible oil of the algorithmic society,[42] their accumulation and processing by private actors has complemented the economic with political power. Technological evolutions, combined with a liberal constitutional approach at the end of the last century across the Atlantic, has led online platforms to set their standards and procedures on a global scale and eroding areas of powers traditionally vested into public authorities. 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

Pelino, 'L'anonimato su internet', in Giusella Finocchiaro (eds), *Diritto all'anonimato* 296 (Cedam 2008). See also Lara Trucco, 'Identificazione e anonimato in rete' www.metakoine.it.

[35] A. Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461.

[36] Steve Lohr, *Data-Ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else* (Blackstone 2015).

[37] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32, 33.

[38] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75; Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen. Cross-Disciplinary Perspectives* (Springer 2008).

[39] Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper Collins 2019).

[40] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).

[41] Solon Barocas and others, 'Governing Algorithms: A Provocation Piece', SSRN (4 April 2013) <https://ssrn.com/abstract=2245322> accessed 14 December 2019; Caryn Devins and others, 'The Law and Big Data' (2017) 27 Cornell Journal of Law & Public Policy 357.

[42] Michele Loi and Paul-Olivier Dehaye, 'If Data is the New Oil, when is the Extraction of Value from data Unjust?' (2018) 7(2) Philosophy & Public Issues 137.

sovereignty'.[43] These actors have been already named 'gatekeepers' to underline their high degree of control in online spaces.[44] As Mark Zuckerberg stressed, '[i]n a lot of ways Facebook is more like a government than a traditional company'.[45] By implementing Terms of Service and community guidelines, platforms unilaterally establish the grounding values of the community and what rights users have within their digital spaces. Formally, these documents are private agreements between users and platforms. However, substantially, the instruments reflect a process of constitutionalisation of online spaces,[46] made by instruments of private ordering shaping the scope of fundamental rights and freedoms of billions of people by adopting a rigid top-down approach. 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.

Online platforms do not limit just to set the standards of protection of their digital spaces. They are also embodying other functions and tasks normally vested in public authorities, like courts or other jurisdictional bodies. The launch of Facebook's Oversight Board is a paradigmatic example of institutionalising this process.[47] These dynamics lead to the privatisation of fundamental rights protection.[48] While public enforcement has been for a long time the default option, based on the role of public authorities as monopoly holder in the context of fundamental rights adjudication, private enforcement has recently emerged as a new trend, when it comes to protecting fundamental rights in the digital realm.[49] Such privatisation of the protection of rights and liberties is just one of the countless processes witnessing a trend of constitutional democracies to delegate public enforcement to private entities.[50] This form of technological regulation is different from legal regulation. As Hildebrandt underlined, technological regulation is not the result of a

[43] Frank Pasquale, 'From Territorial to Functional Sovereignty: The Case of Amazon' Law and Political Economy (6 December 2017) <https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon> accessed 8 September 2019.

[44] Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24(3) International Review of Computer Law and Technology 263; Jonathan Zittrain, 'History of Online Gatekeeping' (2006) 19(2) Harvard Journal of Law & Technology 253; Scott Burris, Peter Drahos and Clifford Shearing, 'Nodal Governance' (2005) 30 Australian Journal of Law and Policy 30.

[45] Franklin Foer, 'Facebook's war on free will' The Guardian (19 September 2017) < https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will> accessed 2 September 2020.

[46] Edoardo Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2018) International Review of Law, Computers and Technology <https://www.tandfonline.com/ doi/abs/10.1080/13600869. 2018.1475898> 14 September 2019; Luca Belli and Jamila Venturini, 'Private Ordering and the Rise of Terms of Service as Cyber-Regulation' (2016) 5(4) Internet Policy Review (2016) https://policyreview.info/node/441/pdf 12 September 2019.

[47] Kate Klonick, 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) 129(8) The Yale Law Journal 2232; Evelyn Douek, 'Facebook's "Oversight Board:" Move Fast with Stable Infrastructure and Humility' (2019) 21(1) North Carolina Journal of Law & Technology 1.

[48] Marco Bassini, 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) 25(2) European Law Journal 182; Rory Van Loo, 'The Corporation as Courthouse' (2016) 33 Yale Journal on Regulation 547.

[49] Giovanni De Gregorio, 'From Constitutional Freedoms to Powers: Protecting Fundamental Rights Online in the Algorithmic Society' (2019) 11(2) European Journal of Legal Studies 65.

[50] Jody Freeman and Martha Minow (eds), *Government by Contract. Outsourcing and American Democracy* (Harvard University Press 2009).

democratic process, excludes disobedience and do not allow to contest due to lack of transparency and accountability of decision-making.[51]

In the algorithmic society, the implementation of automated decision-making systems for this purpose makes the private actors increasingly unaccountable. Increasingly, private actors exercise their influence over decisions on the development of these technologies promising to globally affect society. These private determination are usually based on their own economic, legal and ethical frameworks.[52] Operational parameters for processing information and data are programmed by developers and, then, implemented by online platforms which, being private actors, are not obliged to pursue any public interest and respect fundamental rights in the lack of any regulation.

The entire framework is even more multifaceted when observing that public actors rely on the private sector as a proxy in the digital environment.[53] A tender for the cloud computing infrastructure of a public administration is a clear example of the critical role of public-private partnership where public and private values inevitably merge in a hybrid contractual framework. Likewise, States usually rely on algorithmic enforcement of individuals' rights online, as the case of the removal of illegal content like terrorism or hate speech.[54] In other words, the intersection between public and private leads to wondering how to avoid that the power of online platforms does not lead public values to be subject to the determinations of private business interests.

The rise of private powers in the information society does not only challenge the protection of fundamental rights, such as freedom of expression, privacy and data protection but also democratic values. This constitutional concern can be observed from two perspectives. Firstly, democracy and fundamental rights are intimately intertwined.[55] Among different angles, it is worth observing that, when new technologies raise threats for fundamental rights, especially, civil and political liberties, they are also raising concerns for democratic values. Without expressing opinion and ideas freely, it is not possible to define society as democratic. Likewise, without rules governing the processing of personal data, individuals could not express their identity fearing a regime of private surveillance and they could not rely on a set of accountability and transparency safeguards avoiding the marginalisation of individuals in opaque spheres of data ignorance. Secondly, in the lack of any regulation, the global activity of online platforms contributes to producing a para-legal environment on a global scale competing with States' authority. The consolidation of these areas of private powers is a troubling process for democracy and the rule of law. Even if, at first glance, democratic States are open environments for pluralism flourishing through fundamental rights and freedoms, at the same time, their stability can be undermined when those freedoms transform into new founding powers overcoming basic principles such as the respect of the rule of law. In this situation, there is no effective form of participation or representation of citizens in determining the rules governing their community. The creation of private legal framework outside any representative mechanism undermines the possibility for

[51] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2016).
[52] Brent Mittelstadt and others, 'The ethics of algorithms: Mapping the debate' (2016) 3 Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679> accessed 28 May 2020.
[53] Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 Brookling Law Review 105.
[54] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598.
[55] Luigi Ferrajoli, *Diritti fondamentali. Un dibattito teorico* (Laterza 2001).

citizens to participate in the democratic designing of the law governing their society. In other words, the information society challenges one of the pillars of democratic systems, namely making laws chosen by the people.

Within this framework, individuals find themselves in a situation resembling a new digital *status subjectionis*. Online platforms can autonomously express their authority over a community of billions of individuals. When users enter into an agreement with platforms, they have limited power of negotiations. They accept to relinquish their rights and freedom while legitimizing platforms as authorities to manage those rights, thus, resembling, a private social contract. The primary concern is that, unlike in democratic countries, online platforms exercise this power without democratic procedures but as absolute authority. A new form of (digital) private power has now arisen due to the massive capability of processing data and organizing content. Nonetheless, technology is just a mean for mediating relationship of power between humans. Behind algorithms and automated decision-making technologies, there are actors defining the characteristics of these instruments. These technologies are not autonomous or neutral but make decisions about human beings based on principles decided by other human beings. This is why constitutional law can play a critical role in the algorithmic society as a safeguard for individuals' rights and freedoms as well as democratic values. Therefore, the primary challenge involves not only the role of public actors in regulating the digital environment but also the talent of European constitutional law to react against the threats to fundamental rights raised by the consolidation of transnational private powers online, whose global effects increasingly produces local challenges for modern constitutionalism.

3. Reframing Constitutional Law in the Information Society

If the digital environment has been an opportunity to offer cross border services and exercise individual freedoms in a new space where information and data flow, on the other hand, it has also increased the threats for individuals freedoms which are no longer subject just to public authority but also private determinations. Therefore, the constitutional focus does not concern ownership or property of information but how to protect constitutional principles such as the rule of law and fundamental rights like freedom of expression, privacy and data protection while preserving democratic values. In other words, it is about understanding the relationship between law and technology,[56] precisely constitutional law and digital technologies.[57]

[56] Antonio Ruggeri, 'La "federalizzazione" dei diritti fondamentali, all'incrocio tra etica, scienza e diritto' (2019) (2) Rivista di diritto media 14; Giusella Finocchiaro, 'Riflessioni sul rapporto tra diritto e tecnica' (2012) (4-5) Diritto dell'informazione e dell'informatica 831; Natalino Irti and Emanuele Severino, *Dialogo su diritto e tecnica* (Laterza 2001).

[57] Pollicino and Romeo (n 8); Michele Nisticò and Paolo Passaglia (eds), *Internet e Costituzione*, (Giappichelli 2014); Oreste Pollicino and others, *Internet: regole e tutela dei diritti fondamentali* (Aracne 2013); Marco Orofino, 'L'inquadramento costituzionale del web 2.0: da nuovo mezzo per la libertà di espressione a presupposto per l'esercizio di una pluralità di diritti costituzionali' in AA. VV. (eds), *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee* 33 (Maggioli 2013); Pasquale Costanzo, 'Il fattore tecnologico e le sue conseguenze' (2012) (4) Rassegna parlamentare 811; Sergio Niger, 'Internet, democrazia e valori costituzionali' (2012) 153(4) Astrid <http://www.astrid-online.it/rassegna/ 2012/23_02_2012.html> accessed 6 October 2020; Gaetano Azzariti, 'Internet e Costituzione' (2011) (3) Politica del diritto 367; Paola Marsocci, 'Lo spazio di Internet nel costituzionalismo' (2011) (2) costituzionalismo.it <https://www.costituzionalismo.it/lo-spazio-di-internet-nel-costituzionalismo/> accessed 5 October 2020; Stefano Rodotà, 'Una Costituzione per Internet?' (2010)

Technologies have always created opportunities for economic and societal development,[58] while, at the same time, raised new challenges requiring regulators to find a balance between fostering innovation and mitigating risks.[59] In the past, different technologies have been used to achieve and serve different purposes providing, on the one hand, new opportunities and, on the other hand, challenges concerning their use and implementation.[60] Within the framework of the information society, artificial intelligence technologies are examples of the two-fold nature of technology: opportunity and risk. The discretionary implementation of automated decision-making technologies to process information primarily for profits leads to examining to what extent constitutional law can limit the rise of private powers online to protect fundamental rights and democratic values.

At the end of the last century, scholars, opposing liberal and anarchic approaches,[61] have struggled with explaining whether the digital environment can be regulated. For instance, Lessig underlined the relevance of network architecture between four modalities of regulation including the law, market and society.[62] Likewise, Reidenberg focused on technology and communication network as sources of information policy rules consisting of default rules that go beyond law and government regulation.[63] Murray went ever further underlining how the effectiveness of such regulation does not only depend on the modality of regulation (e.g. network architecture) but also the power that each point of the network can exercise over other dots.[64] It was already clear that the Internet would not entirely overcome state regulation. States have indeed proved their ability to regulate the digital environment like in the case of China.[65]

Nonetheless, States are not the only powerful regulators any longer but are just one piece of the fragmented framework of online governance. As Lynskey underlined, 'the Internet can be regulated and Internet governance is no longer the sole purview of the State'.[66] There are new powers interfering and competing with governmental authorities within the digital environment. Online platforms have become more influential. They have developed their functions as proxies or delegated entities of public authorities to enforce public policies online or autonomously

(3) Politica del diritto 337; Carla Di Lello, 'Internet e Costituzione: garanzia del mezzo e suoi limiti' (2007) (4-5) Diritto dell'informazione e dell'informatica 895; Tommaso E. Frosini, 'Tecnologie e libertà costituzionali' (2003) (3) Diritto dell'informazione e dell'informatica 487.

[58] Viktor Mayer-Schönberger, 'The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship' (2010) 6(2) Journal of Law and Policy for the Information Society 153.

[59] Maria Weimar and Luisa Marin, 'The Role of Law in Managing the Tension between Risk and Innovation' (2016) 7(3) European Journal of Risk Regulation 469.

[60] Lyria Bennett Moses, 'How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target' (2013) 5(1) Law, Innovation and Technology 1; Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008).

[61] Johnson and Post (n 15).

[62] Lessig (n 59).

[63] Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997-1998) 76 Texas Law Review 553.

[64] Andrew Murray, 'Internet Regulation' in David Levi-Faur (ed.), *Handbook on the Politics of Regulation* (Edward Elgar 2011).

[65] Ronald Deibert and others, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008).

[66] Orla Lynskey, 'Regulating Platform Power', (2017) LSE Legal Studies Working Paper 1 <http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf> accessed 6 July 2019.

relying on the mix between market power and technological asymmetry.[67] Put another way, the economic power of business actor is now blurred with authority, so the notion of 'power' is meant in a broader sense than the notion of market power used, for example, in competition law.[68] The problem of private power is not just economic but also political. The accumulation of arbitrary authority in the market outside any form of political accountability can be considered a similar exercise of coercive power characterising state actions.[69] When market and democracy meets the risk is that market dynamics could escape democratic oversight could lead to experiencing a severe constitutional threat for the safeguard of constitutional values.

These challenges provide clues about the role of constitutional law in the algorithmic society. In a sense, the mission of modern constitutionalism is, on the one hand, to protect fundamental rights, and, on the other hand, limit the emergence of powers outside any control.[70] Constitutions have been developed with a view of limiting governmental powers and, thus, shielding individuals from interference by public authorities.[71] From a constitutional law perspective, the notion of power has traditionally been vested in public authorities. Constitutions already provide systems of check and balances for limiting public powers. Still, they have not been conceived as a general barrier against the consolidation of para-legal systems or the exercise (rather abuse) of private freedom. On the contrary, constitutions aim to protect pluralism and freedoms of individuals against interferences of public actors while leaving States the task to intervene to ensure that fundamental rights are respected even at the horizontal level between private actors. This constitutional turn from the vertical to the horizontal dimension is what happens in the context of the horizontal application of fundamental rights or when States decide to regulate a specific field by translating constitutional values in legal norms.[72] Nevertheless, both approaches have their drawbacks. Without being exhaustive in this part of the work, it is worth observing how, on the one hand, a general extension of the horizontal effect could undermine legal certainty by increasing the role of judicial power. On the other hand, increasing the role of political power can lead to overregulation which could disproportionately affect other constitutional interests which deserve to be protected at the same time.

In the information society, the primary threats for constitutional democracies do not exclusively come any longer from public authorities but primarily the governance of spaces which formally are private, but exercise functions traditionally vested in public authorities without any safeguard. 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,

---

[67] Micheal Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Viriginia Journal of Law and Technology 6.

[68] Recently, scholars have approached the public role of online platforms from different perspectives. See Natali Helberger and others, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34(1) The Information Society 1; Luca Belli, Pedro A Francisco and Nicolo Zingales, 'Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police' in Luca Belli and Nicolo Zingales (eds), *How Platforms are Regulated and How They Regulate Us* 41 (FGV Rio 2017).

[69] Morris R. Cohen, 'Property and Sovereignty' (1927) 13 Cornell Law Review 8.

[70] Jeremy Waldron, 'Constitutionalism: A Skeptical View' (2012) NYU Public Law Research Paper 10-87 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1722771&rec=1&srcabs=1760963&alg=1&pos=> accessed 14 October 2019.

[71] András Sajó and Renáta Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

[72] Eleni Frantziou, *The Horizontal Effect of Fundamental Rights in the European Union A Constitutional Analysis* (Oxford University Press 2019).

businesses, and civil society organisations'.[73] Put in a different way, digital constitutionalism consists of articulating the limits to the exercise of power in a networked society.[74] This, however, does not imply to revolutionise the grounding roots of modern constitutionalism but rediscover the role of constitutional law in the algorithmic society and interpret its challenges under a digital constitutional perspective.

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 eighteenth century where, according to the Lockean idea, the power of governments should be legally limited, and its legitimacy depends upon complying with these limitations.[75] Despite this chronological gap, the adjective 'digital' entails placing constitutionalism in a temporal and material dimension. Digital constitutionalism indeed refers to a specific timeframe, precisely the aftermath of the Internet at the end of the last century. Moreover, from a material perspective, this adjective qualifies constitutionalism. The focus is on how digital technologies and constitutionalism affect each other. Therefore, the merger of the expressions 'digital' and 'constitutionalism' does not lead to revolutionise the pillars of modern constitutionalism. Instead, it aims to understand how to interpret the role of constitutional law in the information society. Digital constitutionalism contributes to fostering a democratic constitutional narrative in the digital environment. By defining a new theoretical and practical field based on a dynamic dialectic between how digital technologies affects the evolution of constitutionalism, digital constitutionalism can show how constitutional law reacts against the power emerging from digital technologies implemented by public and private actors. In other words, digital constitutionalism is about reframing the protection of fundamental rights and the exercise of powers in the digital environment. In this work, this process of reframing modern constitutionalism in the information society is named 'digital constitutionalism'.

4. The Forgotten Talent of European Constitutional Law

This situation can be considered a way to test the talent of European constitutional law before the challenges of the information society. The primary concern is whether the characteristics of European digital constitutionalism could fit within the purposes of facing the consolidation of private powers online undermining constitutional principles, precisely the rule of law, the protection of fundamental rights and the safeguards for democracy.

The Union is a paradigmatic example of the constitutional reaction to the challenges of the information society. From a liberal imprinting at the end of the last century, the policy of the Union in the field of digital technologies has shifted to a constitutional-based approach. The role of European Courts and the steps taken by the Commission with the Digital Single Market strategy are examples of this shift of paradigm. This change of heart has been constitutionally

[73] Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press, 2019), 173.
[74] Claudia Padovani and Mauro Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System* (2018) 80 International Communication Gazzette 295.
[75] Andras Sajò and Renata Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

driven by transnational corporations performing quasi-public functions on a global scale, thus, competing with public actors and imposing their standards of protection of fundamental rights.[76] 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 online platforms, which, although vested as private actors, increasingly perform quasi-public tasks. The freedom to conduct business enshrined in the Charter of Fundamental Rights ('Charter') has now turned into a new dimension,[77] namely that of private power, which brings significant challenges to the role and tools of constitutional law. It is because of new automated technologies based on algorithmic technologies if this freedom has turned into power. If Google and Facebook can rely on a set of information able to gather more information than traditional public authorities, it should not surprise if they can exercise a form of power which can compete if not overcome in some cases that of public authorities. If they can establish standards of protection of users' rights on a global scale, we should not be surprised by potential concerns for the rule of law and democratic values. The acceptance of these challenges would lead to vanish constitutional values and replace them with logics reflecting market interests.[78]

This new constitutionally oriented season triggered by the talent of European constitutional law to react against the emergence of private powers in the information society is the result of a framework of dignity that do not tolerate that a liberal approach or democratic tolerance can be exploited to destroy democracy itself.[79] Since the horror of the Second World War, European states started to incorporate and codify human dignity within its founding values.[80] The post-war scenario was a decisive moment for the emergence of dignity as a European constitutional principle,[81] thus, elevating to 'cornestone of the postwar constitutional state'.[82] Besides, dignity is not an isolated concept but a foundational principle connected with the values and aspirations shaping European constitutionalism. Also driven by the international framework, human dignity has started to emancipate the eastern side of the Atlantic from the western where the liberal imprinting of constitutional law still remains the primary foundation of fundamental rights and liberties.[83] Indeed, the consolidation of human dignity at the international level is evident even when focusing on the European regional level, precisely the European Convention on Human Rights ('Convention').[84] The Strasbourg Court considers human dignity as underpinning values protecting all the other rights of the Convention.[85]

---

[76] Oreste Pollicino and Giovanni De Gregorio, 'A Constitutional Driven Change of Heart. ISP Liability and Artificial Intelligence in the Digital Single Market' 18(1) The Global Community Yearbook of International Law and Jurisprudence 238.
[77] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.
[78] Rodotà (n 25).
[79] Christine Duprè, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Hart 2015).
[80] Paolo Becchi and Klaus Mathis (eds), *Handbook of Human Dignity in Europe* (Springer 2019).
[81] James Q Whitman, 'On Nazi 'Honour' and the New European 'Dignity', in Christian Joerges and Navraj Singh Ghaleigh (eds), *The Darker Legacies of Law in Europe* (Hart 2003), 243.
[82] Lorraine Weinrib, 'Human Dignity as a Rights-Protecting Principle' (2004) 17 National Journal of Constitutional Law 330.
[83] Giovanni Bognetti, 'The Concept of Human Dignity in European and U.S. Constitutionalism' in Georg Nolte (ed.), *European and US constitutionalism* (Cambridge University Press 2005), 95.
[84] Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19(4) European Journal of International Law 655.
[85] Pretty v United Kingdom (1997) 24 EHRR (1997) 423, 65.

The influence of the Council of Europe and Member States can be understood even when moving to the framework of the Union. In *Omega*, the European Court of Justice ('ECJ') held that 'the Community legal order undeniably strives to ensure respect for human dignity as a general principle of law'.[86] Likewise, the ECJ recognised human dignity as part of the Member States' public security and order.[87] The recognition of human dignity as a general principle of law before the entry into force of Charter of Fundamental Rights of the European Union ('Charter') is an evident example of the consolidation of the process of European cosntitutionalisation to which the ECJ opened the door since *Stauder*,[88] as also evolved in *Internationale Handelsgesellschaft* and *Nold*.[89] In addition, human dignity is established as the first and separate human rights in the Charter. Its primacy and autonomy would suggest its role as overarching principle but also as a fundamental right which does not leave room for any interference. Indeed, human dignity is not just enshrined in the preamble of the Charter, but it is protected as a separate and inviolable fundamental right.[90] Even if the Charter would provide the possibility to limit fundamental rights,[91] a systematic interpretation would reveal that this does not apply to human rights with absolute protection as those protected by the ECHR.[92] Therefore, even in the lack of accession of the Union's system to the ECHR, it is still possible to define an intimate bundle which characterises human dignity as the overarching principle of European constitutionalism.

The Lisbon Treaty has recognised the role of human dignity as a pillar of European constitutionalism. Even if the preamble of the Treaty of the European Union ('TEU') just mentions human rights and the inalienable rights of human persons,[93] human dignity has been enshrined as the first of the common values of the Union.[94] The position in EU primary law is not neutral but constitutes a legal obligation to respect this human right for public actors and an objective driving all the Union's activities. Besides, the recognition of the Charter as a source of EU primary law has led to the consolidation of the European constitutional framework with the result that human dignity has become a mandatory point of reference within the European constitutional framework.

Within this framework, dignity is not only an objection or a fundamental right but a promise for democracy after a phase of dehumanisation. Human dignity as a constitutional foundation is the result of the process of the European experience whose values aim to foster a vision of democracy where human beings can take decisions on their life and shape collective decisions. Human dignity is not just avoiding torture or ensuring equality, but it is the constitutional foundations of European democratic values which protects fundamental rights and provide institutions to achieve this purpose. Therefore, human dignity also aims to achieve a utopian goal

[86] Case C–36/02, Omega Spielhallen und Automatenaufstellungs- GmbH v Oberbürgermeisterin der Bundesstadt Bonn (2004) ECR I–9609, 34.
[87] Joined Case C-331/ 16 and C-366/16, K. v Staatssecretaris van Veiligheid en Justitie and H.F. v Belgische Staat (2018), 47.
[88] See Case 29/69, Erich Stauder v City of Ulm - Sozialamt (1969).
[89] Case 11/70, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel (1970); Case 4/73, J. Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft (1977).
[90] Charter (n 77), Art 1. See also Art 25, 31.
[91] Ibid, Art 52.
[92] Ibid, Art 52(3).
[93] Treaty on the European Union (2012) OJ 326/13, preamble 2, 4.
[94] Ibid, Art 2.

while driving European constitutionalism towards individuals as the core of fundamental rights protection and critical part of democracy. As observed, 'there is no foolproof constitutional design that can immunise liberal democracy from the pressures of backsliding. At best, constitutional design features serve as speed bumps to slow the agglomeration and abuse of political power; they cannot save us from our worst selves completely'.[95] This risk does not concern only political or external forces which aim to overthrown democratic safeguards but also the interferences of private powers whose activities are backed by a liberal constitutional approach. The predominance of digital capitalism pushes human dignity to express its role as the beacon and the overarching framework of the European constitutional systems. European digital constitutionalism should not be seen as a mere reaction, but the need to avoid that constitutional values are not put aside by private business interests. Put another way, it is also a proactive approach rather than just a firm reaction to the potential vanishing of democratic values.

Therefore, this situation leads to wondering about the role of European constitutional law before these challenges. While the Union framework is at the forefront of a new constitutional approach to private powers online, the US seems following an opposite path. Both in the field of content and data, in the last twenty years, the US policy adopted an 'omissive' approach based on a First Amendment dogma. Still, the responsibilities of online platforms' activities is based on a legal framework adopted at the end of the last century based on immunity and exemption of liability.[96] In the field of data, apart from some national attempts,[97] there is not a harmonised approach at federal level to privacy and data protection. Moving from the Congress to the Supreme Court, even in this case, there has been a restrictive approach towards any public attempt to regulate the digital environment,[98] or horizontal extension of constitutional obligations.[99] At first glance, the executive order on preventing online censorship adopted in 2020 would seem a turning point towards more control online.[100] However, the concrete effects of this constitutional paradox on the digital environment are still to be examined.[101]

These non-exhaustive considerations on the constitutional approaches of the other side of the Atlantic anticipate that digital constitutionalism, as an expression of modern constitutionalism, should not be seen as a monolith. It is intimately connected with the constitutional framework of each legal and political system. The rise of digital constitutionalism across the Atlantic is the result of paths guided by different constitutional premises. The European constitutional reaction to the challenges raised by private actors is not the general rule. In the last twenty years, the US framework has not reacted to the rise of private powers but highly defended the concept of liberty stoned in the protection of the First Amendment. The liberal approach of the US could also be

---

[95] Tom Ginsburg, Aziz Z. Huq and Mila Versteeg, 'The Coming Demise of Liberal Constitutionalism?' (2018) 85(2) The University of Chicago Law Review 239, 253.

[96] Communications Decency Act (1996), Section 230; Digital Millennium Copyright Act (1997), Section 512.

[97] See, e.g., California Consumer Privacy Act (2020).

[98] See, e.g., Packingham v North Carolina, 582 U.S. ___ (2017).

[99] See, e.g., Manhattan Community Access Corp. v Halleck, No. 17-1702, 587 U.S. ___ (2019).

[100] Executive Order on Preventing Online Censorship (28 May 2020) <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> accessed 8 June 2020.

[101] Giovanni De Gregorio and Roxana Radu, 'Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech' MediaLaws (6 June 2020) <http://www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/> accessed 10 June 2020.

considered another expression of digital constitutionalism showing a different talent of US constitutional law which looks at online platforms as an enabler of liberties and democracy rather a threat to such values. Such a framework of liberty has been increasingly abandoned on the eastern side of the Atlantic where the different constitutional humus based on human dignity have paved the way towards a new constitutional moment.[102]

Looking at the eastern side of the Atlantic, the challenges raised by the power of private actors in the digital environment lead to question the traditional boundaries of constitutional law to understand to what extent the European talent can remedy to the current situation of threat for fundamental rights and democracy. Digital constitutionalism can indeed provide the instruments to deal with platforms' powers as well as the guiding principles and remedies to restore the constitutional equilibrium. This is the primary mission of digital constitutionalism consisting of framing and extending constitutional values in the algorithmic society.

4. Investigating European Digital Constitutionalism

This research aims to capture the emergence of a new season for constitutionalism in the Union (i.e. digital constitutionalism). This new phase is examined in a two twofold way. Firstly, this work investigates the reasons leading to this new constitutional moment in the Union. Secondly, it provides a normative framework analysing how and to what extent European constitutional law can remedy the situation of imbalances of powers threatening fundamental rights and democracy in the algorithmic society. This descriptive and normative framework provides a picture of the role of European constitutional law in the algorithmic society, especially by focusing on the intersection between freedom of expression, privacy and data protection.[103] The primary goal is to examine how European digital constitutionalism can provide legal instruments to address the challenges raised by transnational private actors operating in the digital environment. Although the challenges coming from the implementation of these technologies also involve public actors, this research underlines that the reaction of European digital constitutionalism is primarily the result of the threats to fundamental rights and democratic values coming from the rise of private powers in the information society.

Within this framework, the first question to answer is: what are the reasons for the rise of European digital constitutionalism? Some scholars have introduced a new constitutional moment,[104] mapped bill of rights and legislative attempts concerning the relationship between Internet and constitutions.[105] Outside Europe, Fitzgerald stressed that the exercise of power is

[102] James Q. Whitman, 'On Nazy "Honour" and the New European Dignity' in Christian Joerges and Navraj Singh Ghaleigh, *Darker Legacies of Law in Europe: The Shadow of National Socialism and Fascism Over Europe and Its Legal Traditions* (Hart 2003).
[103] For an Australian perspective, see Monique Mann, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia' (2018) 80 International Communication Gazette 369.
[104] Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorization' (2019) 33(1) International Review of Law, Computers and Technology 76.
[105] Dennis Redeker, Lex Gill and Urs Gasser, 'Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights' (2018) 80(4) International Communication Gazette 302; Mauro Santaniello and others, 'The Language of Digital Constitutionalism and the Role of National Parliaments' (2018) 80 International Communication Gazette 320.

shared between public and private actors in the information society.[106] The mediation between powers and freedom involves the relationship between both sides of the same coin. According to Fitzgerald, the information society is a specific example of this strict connection. The characteristics of the digital environment like decentralisation led to a mix of governance in search of a balance between public intervention and private self-regulation. The idea of Fitzgerald is that 'information constitutionalism' as the law of the State should delimit the boundaries of self-regulation through which private actors determine their standards manipulating software (*rectius* technological architecture). Therefore, it is private law which is called to solve the challenges of the information society through the guidelines of constitutional values.

Likewise, Berman acknowledged the role of private actors in defining and use the code of the cyberspace to regulate the digital environment.[107] It was one of the first scholars, together with Boyle,[108] that question the role of sovereignty and power online from a public law standpoint. Berman proposed an approach towards 'constitutive constitutionalism' consisting of the possibility to open constitutional adjudication to private actors as a mean to overcome the vertical dimension of the state action in US constitutional law and allow judges and individuals to address these pressing issues. More recently, Suzor underlined that the power relationship in the information society should be governed by public principles and platforms' legitimacy should be assessed through the lens of the rule of law.[109] According to Suzor, the project of digital constitutionalism is 'to rethink how the exercise of power ought to be limited (made legitimate) in the digital age'.[110]

Building on this framework, this contribution is more ambitious since it would be the first attempt to root a digital constitutional analysis within a specific constitutional framework, especially in the European context. The debate neglected the role of constitutional law as a shield against emerging powers online in Europe. This is also the heritage of a long debate about the regulatory powers of states over the Internet where the role of constitutional law has not been investigated. Rather than understanding the influence of constitutional systems and values in the digital environment, libertarian and paternalistic answers have focused more on how to ensure an effective regulation looking at the technological dimension outside any specific constitutional framework of reference. Even if there are several works addressing the impact of digital technologies over fundamental rights,[111] still, there is not a systematic constitutional perspective on how to address the challenges raised by private powers in the algorithmic society.

---

[106] Brian Fitzgerald, 'Software as Discourse - A Constitutionalism for Information Society' (1999) 24 Alternative Legal Journal 144.

[107] Paul S. Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 University of Colorado Law Review 1263.

[108]James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' (1997) 66 University of Cincinnati Law Review 177.

[109] Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) Social Media + Society, 4 <https://journals.sagepub.com/doi/pdf/10.1177/ 2056305118787812> accessed 27 November 2019.

[110] Ibid, 4.

[111] Mireille Hildebrandt and Kieron O'Hara (eds), *Life and the Law in the Era of Data-Driven Agency* (Edward Elgar 2020); Ben Wagner and others (eds), *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations* (Edward Elgar 2019); Pollicino and Romeo (n 8); Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Cavendish 2005).

Investigating the rise and consolidation of European digital constitutionalism cannot neglect the analysis of online platforms' powers. This is why the second research question is: what are the characteristics and the limits of platforms' powers in the digital environment? Answers to this question are still fragmented, and there is a lack of attention to the notion of 'power' of online platforms from the standpoint of constitutional law. So far, scholars have focused on powers from different perspectives. This term has been interpreted as market power in the context of competition law,[112] imbalances of power in the field of consumer law,[113] and even 'data power' in the field of data protection.[114] The way in which these three areas looks at the notion of power is not homogenous. Power is defined from an economic perspective which fails to provide a constitutional analysis of the threats coming from the consolidation of market powers increasingly going public. Competition, contract law and consumer law only provide one side of the coin, especially that of the internal market. Indeed, they fail to picture the evolution of the Union as a polity.[115] In other words, the lens of competition, contract and consumer law fails to address the other side of the coin which digital constitutionalism represents. This shift of attention does not imply that the aforementioned legal framework cannot participate in the puzzle of platforms' powers. Nonetheless, these remedies cannot be left alone without the guidance of constitutional law any longer. This research aims to fill this gap. Precisely, this work defines two forms of powers, namely delegating and autonomous powers resulting from the mix of the liberal constitutional approach adopted by the Union at the end of the last century and the exploitation of private law and new technologies by online platforms to consolidate new areas of power beyond economic freedoms.

The primary challenge in the algorithmic society is to avoid that private powers impose their standards of protection replacing constitutional values with unaccountable determinations. The role of constitutional law is critical to define the path to inject democratic values in a free-market environment. This approach does not imply that public intervention should guide market dynamics. The free-market approach could be enriched (and not threatened) by public safeguards which avoid to forgot that neglecting the role of constitutional law for achieving internal market goals has contributed to consolidating the situation of imbalances of powers and threats to democratic values constitutional democracies are facing in the information society. Leaving broad margins of discretion to private actors has led to transforming their freedoms into new founding powers without system of public oversight to ensure transparency and accountability.

---

[112] See, e.g., Nicolas Petit, *Big Tech and the Digital Economy. The Moligopoly Scenario* (Oxford University Press 2020); Viktoria H.S.E. Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57(1) Common Market Law Review 161; Damien Geradin, 'What Should EU Competition Policy do to Address the Concerns Raised by the Digital Platforms' Market Power?' (2018) TILEC Discussion Paper No. 2018-041 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3011188> accessed 2 October 2019; Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility: Data as Essential Facility* (Wolter Kluwer 2016); Angela Daly, *Private Power, Online Information Flows and EU Law. Mind the Gap* (Hart 2016); Daniel Zimmer, 'Digital Markets: New Rules for Competition Law' (2015) 6(9) Journal of European Competition Law & Practice 627.

[113] See, e.g., Christoph Busch and others, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 5 Journal of European Consumer and Market Law 3.

[114] Orla Linskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 (1) Theoretical Inquiries in Law 189.

[115] Massimo Fichera, *The Foundations of the EU as a Polity* (Edward Elgar 2018).

Therefore, it is time to shed light on the role of European constitutional law as a shield against the exercise of private powers in the digital environment. This constitutional analysis of platforms' powers deserves to be analysed at least from a regional perspective. It is worth stressing that constitutional law reflects the values and principles of a certain society. Even if constitutional principles are shared at the global level and intertwine with international law,[116] still, the way in these principles are interpreted and implemented is influenced by local dynamics, institutional design and understanding of constitutional protection. This is evident when looking at the protection of fundamental rights across the Atlantic, especially the right to freedom of expression.[117]

The focus on the European framework is critical for this research not only to anchor the analysis to a specific constitutional area but also for answering the third research question: which remedies European constitutional law can provide to solve the imbalances of power in the algorithmic society and mitigate the risks for fundamental rights and democratic values? This is a matter of how European constitutionalism protects fundamental rights and principles like the rule of law and citizens' participation.[118] While, from a constitutional law perspective, power has traditionally been vested in public authorities, a new form of (digital) private power has now come into play determining standards of protection and procedures based on their social, legal and ethical framework.

This work argues that the protection of fundamental rights and democratic values is no longer a matter of 'quantity'. The quantitative perspective has shown its failure in the last years when looking at the attempts to codifying Internet constitutions. Internet advocacy organisations and scholars have called and analysed the adoption of Internet bill of rights. Many propositions have been made in this respect,[119] and even public authorities tried to follow this path like in Brazil and Italy.[120] The failure of establishing a general right to Internet access at the constitutional level is a clear example that it is necessary to work with the instruments that constitutional law already provides to lawmakers and judges.[121] Besides, these calls for more constitutional protection have

---

[116] Jan Klabbers, Anne Peters and Geir Ulfstein, *The Constitutionalisation of International Law* (Oxford University Press 2008).

[117] Vincenzo Zeno-Zencovich, *Freedom of Expression: A Critical and Comparative Analysis* (Routledge 2008).

[118] Joseph H. H. Weiler and Marlene Wind (eds), *European Constitutionalism beyond the State* (Cambridge University Press 2003).

[119] Redeker, Gill and Gasser (n 105).

[120] Marco Civil da Internet, Law no. 12.965 (2014); Dichiarazione dei diritti in Internet (2015). Maria R. Allegri and Guido d'Ippolito (eds), *Accesso a Internet e neutralità della Rete, tra principi costituzionali e regole europee* (Aracne 2017); Tommaso E. Frosini, 'Il diritto di accesso ad Internet', in Tommaso E. Frosini and others (n 10).; Oreste Pollicino and Marco Bassini, *Verso un Internet Bill of Rights* (Aracne 2015); Marina Pietrangelo (eds), *Il diritto di accesso ad Internet* (Edizioni Scientifiche Italiane 2011); Lorenzo Nannipieri, 'Costituzione e nuove tecnologie: il caso dell'accesso ad Internet' (2013) Gruppo di Pisa <https://www.gruppodipisa.it/images/rivista/pdf/Lorenzo_Nanniperi_-_Costituzione_e_nuove_tecnologie_profili_costituzionali_dell_accesso_ad_Internet.pdf> accessed 4 October 2020; Pasquale Costanzo, 'Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)' (2012) Consulta Online < http://www.giurcost.org/studi/Costanzo15.pdf> accessed 4 October 2020; P. Tanzarella, 'Accesso a Internet: verso un nuovo diritto sociale?' in Elisa Cavasino, Giovanni Scala and Giuseppe Verde, *I diritti sociali dal riconoscimento alla garanzia: il ruolo della giurisprudenza* (Editoriale scientifca 2012).

[121] Oreste Pollicino, 'Right to Internet Access: Quid Iuris?' in Andreas von Arnauld, Kerstin von der Decken and Mart Susi (eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric* 263 (Cambridge University Press 2019); Stephen Tully, 'A Human Right to Access the Internet? Problems and

not led to concrete solutions to face the constitutional challenges of the algorithmic society. Traditional bills of rights do not allow to remedy the transparency and accountability gap which individuals suffer from in their relationship with private actors that implement algorithms on a larger scale.

Therefore, this work does not propose introducing new constitutional rights but focuses on the 'quality' of protection. It is not the first time that scholars focus their attention on private actors' ability to interfere with individuals' fundamental rights as a threat to constitutional states. A traditional answer given to this challenge has been the horizontal effects doctrine,[122] or state action doctrine in the US framework.[123] The background idea is to extend the scope of application of the existing bills of rights and human rights covenants to horizontal relationships (i.e. between private parties). In the case of online platforms, the horizontal effect doctrine could look like a potential leeway to require these actors to comply with constitutional safeguards.[124] Nevertheless, even if the horizontal application of freedom of expression and data protection could be a first step to protect individuals' rights, it would be not enough due to its case-by-case structure which could undermine the principle of legal certainty if extensively and incoherently applied, especially in civil law countries where there is not a system based on the common law principle *stare decisis*.

It is then necessary how the need to protect fundamental rights and democratic values can lead to a positive obligation for public actors to intervene in the field of content and data. Scholars have failed to capture this constitutional angle. For instance, recently scholars have focused on the right not to be subject to an automated decision-making process, established by Article 22 of the GDPR,[125] or how to address the issues of content moderation.[126] These two cases have

---

Prospects' (2014) 14(2) Human Rights Law Review 175; Paul de Hert and Darek Kloza, 'Internet (Access) as a new Fundamental Right. Inflating the Current Rights Framework?' (2012) 3(2) European Journal of Law and Technology <http://www.ejlt.org/index.php/ejlt/article/view/123/268> accessed 2 October 2020; Nicola Lucchi, 'Freedom of Expression and the Right to Internet Access', in Monroe E. Price, Stefaan G. Verhulst, Libby Morgan (eds), *Routledge Handbook of Media Law* (Routledge 2013).

[122] Sonya Walkila, *Horizontal Effect of Fundamental Rights in EU Law* (European Law Publishing 2016); Dorota Leczykiewicz, 'Horizontal Application of the Charter of Fundamental Rights' (2013) 38(3) European Law Review 479; Elena Gualco and Luisa Lourenço '"Clash of Titans". General Principles of EU Law: Balancing and Horizontal Direct Effect' (2016) 1(2) European Papers 643; Eleni Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (2015) 21(5) European Law Journal 657.

[123] Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1(1) International Journal of Constitutional Law 79; Stephen Gardbaum, 'The Horizontal Effect of Constitutional Rights' (2003) 102 Michigan Law Review 388.

[124] Jonathan Peters, 'The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms' (2018) 32 Berkeley Technology Law Journal 988. See also Berman (n 107).

[125] Andrew D. Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Margot E. Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkley Technology Law Journal 189; Sandra Wachter and others, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Gianclaudio Malgieri and Giovanni Comandè, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 234; Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.

[126] Klonick (n 54); Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018); Kyle Langvardt, 'Regulating Online Content Moderation' (2018) 106 The Georgetown Law Journal 1353.

triggered a debate on whether individuals can rely on effective rights to protect themselves from potentially harmful consequences of the implementation of algorithms. This debate is an important part of the jigsaw and deserves to be enriched by constitutional guidelines to deal with the challenges of the algorithmic society in the next decades. The issue of the right to explanation is just the beginning of a series of issues questioning traditional legal categories and how fundamental rights are conceived and protected. The sole right to explanation, in fact, cannot remedy the asymmetry between individuals and algorithms. This work aims to fill this gap underlining how constitutional law can lead to a more systematic strategy to address the issues of the algorithmic society.

To complete the analysis of European digital constitutionalism, it is worth focusing on a fourth research question: which paths the consolidation of European digital constitutionalism could open to the Union in the next years? The rise of the algorithmic society has already highlighted some constitutional challenges which the Union will be called to address in the next future. It is worth wondering how to balance innovation in the internal market and the need to ensure sustainable development of new technologies able to protect fundamental rights and freedoms which are already under pressure. This question would focus on understanding whether European constitutionalism would lead to a predominance of the free market approach as at the beginning of the next year following the promises of artificial intelligence technologies (i.e. digital capitalism) or will learn from the past by adopting a cautious strategy aimed to protect individuals' rights and freedoms (i.e. digital humanism). The Union has already shown its intention to focus on ethics and a human approach in the field of artificial intelligence.[127] This political crossroads deserves particular attention in this research since this choice will be critical not only for the growth of the internal market but also for the protection of constitutional values, especially human dignity, in the long run.[128]

A second point would focus on the dilemma between regulation and self-regulation, thus, leading to wondering how these approaches can better ensure to implement public policies online ensuring innovation while protecting fundamental rights and democratic values. Under the Digital Single Market strategy, the Union has already implemented hard and soft legal measures.[129] Nevertheless, the increasing predominance of artificial intelligence technologies could indirectly force the Union to adopt liberal approaches not to hinder the development of these technologies and not to bind forces with increasingly political power coming from a combination of economic and technological power.

Besides, there is increasing attention on the extraterritorial scope of fundamental rights, especially in the field of data.[130] This is not a trivial question since the cases of clashes of fundamental rights protected by different constitutional framework can shape the degree of protection through extraterritorial conflicts. Therefore, understanding the boundaries of

[127] High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 2 December 2019.
[128] White Paper, 'On Artificial Intelligence - A European Approach to Excellence and Trust' COM(2020) 65 final.
[129] Pollicino and De Gregorio (n 76).
[130] Paul de Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6(3) International Data Privacy Law 230, 240; Christoper Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235.

extraterritoriality of fundamental rights' protection is crucial to underline the potential path of digital constitutionalism in the Union.

To answer these research questions, this research follows a precise methodology. Firstly, the focus is on the European framework, precisely investigating digital constitutionalism within the framework of the Union and the Council of Europe. The research also takes into account the role of Member States at national level within the supranational analysis. Likewise, a comparative approach with the US framework is also embedded in this research without, however, losing its European focus. The reference to the US legal framework is critical to this research due to the influence and interrelation between the two constitutional systems in the information society. Secondly, another methodological pillar consists of taking the challenges for freedom of expression, privacy and data protection in the algorithmic society as paradigmatic examples. This two-fold analysis is present in all the chapters of the work showing the impact of private powers on two of the most critical fundamental rights in the digital environment. As already stressed, this should not surprise since freedom of expression and data protection are two democratic cornerstones. In the information society, without expressing ideas and opinion openly or accessing instruments of transparency and accountability concerning the protection of personal data, democracy is just a label failing to represent a situation of veiled authoritarianism. Thirdly, the research addresses the topic of digital constitutionalism from a descriptive to a normative perspective. The mix between these two standpoints allows firstly to understand the grounding framework on which the normative argument is built. Describing the reasons leading to the rise of European digital constitutionalism becomes a preliminary basis to address the normative part of the research, precisely which remedies European constitutional law can provide to address the challenges of the algorithmic society like in the cases of content moderation and automated decision-making processing of personal data.

5. Structure of the Research

This work is articulated in two parts. After this introductory chapter, Chapters II-IV describe the path leading to the rise of digital constitutionalism in the Union, the ability of platforms to exercise delegated and autonomous powers in the digital environment as well as the intimate relationship between expressions and personal data in the algorithmic society. This descriptive frame provides the grounds on which the normative claims are supported in Chapters V-VI. These focus in particular on how to address the challenges raised by the private powers implementing artificial intelligence technologies to freedom of expression and data protection by analysing the constitutional challenges of content moderation and automated decision-making processes based on personal data. The last chapter provides potential interpretations of the possible paths of European digital constitutionalism, precisely underlining three critical challenges raising questions whose answers can be found through the digital constitutional lens provided by this research.

Chapter II focuses on the rise of digital constitutionalism in the Union. It focuses on the evolution of the Union's approach to regulate the flow of expressions and data online since the end of the last century. This path is described in three constitutional phases: digital liberalism, judicial activism and digital constitutionalism. The first season illustrates how, in the aftermath of the Internet, the liberal approach concerning online intermediaries and data protection was

rooted in the fear to overwhelm the market and slow the development of new digital products and service which promises to promote the economic growth. 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 European standpoint from fundamental freedoms to fundamental rights. This second phase has only anticipated a new phase of European constitutionalism (i.e. digital constitutionalism) based on codifying the ECJ's case law and limiting online platforms' powers within the framework of the Digital Single Market.

Chapter III examines how platforms perform functions in a way resembling the exercise of public authorities. It would be not enough to explain the reasons for the rise of digital constitutionalism without explaining how platforms express private powers. This chapter divides platforms' powers into two categories: delegated powers and autonomous powers. Despite the distinction, these two forms of power are interrelated. The first category includes functions which platforms exercise according to the delegation of public authorities. In this case, it would be possible to define legislative and judicial delegation of powers. The acknowledgement of online platforms' role to police content in case of awareness or the enforcement of the right to be forgotten online can provide two examples of how powers have shifted from the public to the private sector. Nothing new so far unless for the lack of any public safeguard in the delegation of these powers that could avoid the extension of these function into forms of autonomous powers. In these cases, platforms have shown to be able to define and enforce the rule of their communities while also exercising a balancing activity between the fundamental rights at stake. These autonomous powers contribute to defining a para-legal framework where users are subject to a new *status subjectionis* in relation to private power which does not know separation of functions or democratic processes, thus, resembling authoritarian regimes.

Before to focus on the challenges of content moderation and automated decision-making in the field of data, Chapter IV deals with another crucial piece of the puzzle: the overlapping layers between content and data in the algorithmic society. This chapter shows how these two fields guiding this research are not isolated in the information society. There is an intimate interrelation between the legal and technological regime governing content and data explaining their role. Their legal regimes have been conceived on parallel tracks. The rise of the algorithmic society has blurred this traditional gap, thus, increasing the technological convergence between content and data. From a merely passive role, new online intermediaries such as search engines and social networks have acquired an increasingly active role in managing online content. At the same time, their role in deciding how to process personal data has transformed these actors from data processors to controllers. This evolving framework from passive to active intermediaries has led to the convergence of the parallel tracks which have started to overlap. The rise of the algorithmic society has contributed to reducing the technological distance between expressions and data and increasing the need to increase the legal convergence of content and data to protect democratic values against abuse of powers.

Chapter V introduces the normative part analysing the challenges in the field of content moderation. Although freedom of expression is one of the cornerstones on which democracy is based, this statement firmly clashes with the troubling evolution of the algorithmic society where artificial intelligence technologies govern the flow of information online according to opaque technical standards established by social media platforms. Nonetheless, the chapter shows how

these actors are usually neither accountable nor responsible for contents uploaded or generated by the users. Therefore, the chapter argues that the liberal paradigm of protection of the right to free speech is no longer enough to protect democratic values in the digital environment, since the flow of information is actively organised by business interests, driven by profit-maximisation rather than democracy, transparency or accountability. Although the role of free speech is still paramount, it is necessary to focus on the positive dimension of this fundamental right by establishing new users' rights in online content moderation to protect democratic values and foster media pluralism online.

Likewise, Chapter VI deals with the other side of the coin consisting of the use of artificial intelligence systems to process personal data. The chapter underlines how the characteristics of this kind of processing highly challenge the protection of personal data which raised as an answer to the development of new digital technologies. The chapter firstly describes the clash between data protection values and artificial intelligence systems underlining tensions and potential safety valves. Then, the chapter examines how automated decision-making processes should be read in light of the constitutional framework of data protection whose values are rooted in democratic principles like the rule of law, proportionality and due process. Unlike in the field of content, in this case, the primary issue is not the lack of safeguard but their interpretation which should focus on the aim of constitutional values to protect democratic values while balancing the need to promote the growth of the internal market.

Once the work describes the reasons for the rise of European digital constitutionalism as an answer to private powers online and the constitutional remedies to address this situation, Chapter VII focuses on the potential path of European digital constitutionalism by analysing three challenges: digital humanism v digital capitalism; public authority v private ordering; extraterritoriality v constitutional protectionism. The chapter does not focus on these poles as trade-offs but underlines how the characteristics of European digital constitutionalism would lead to a sustainable approach between these global trends. It provides potential paths, thus, defining the characteristics of a new phase of European digital constitutionalism in the algorithmic society.

Chapter II

The Rise of Digital Constitutionalism in the European Union

Summary: 1. From Digital Liberalism to Digital Constitutionalism. – 2. The First Phase: Digital Liberalism. 2.1 Exempting Online Intermediaries from Liability. 2.2 Ensuring the Free Circulation of Personal Data. – 3. The Second Phase: Judicial Activism. 3.1 From Economic Interests to Fundamental Rights. 3.2 The Judicial Path towards Digital Privacy. – 4. The Third Phase: Digital Constitutionalism. 4.1 Safeguards in Content Moderation. 4.2 Safeguards in the Algorithmic Processing of Personal Data. – 5. Freedoms and Powers in the Digital Environment.

1. From Digital Liberalism to Digital Constitutionalism

The rise and consolidation of European digital constitutionalism cannot be understood without focusing on the path which the Union has run across the last twenty years. The approach of the Union has shifted from a liberal perspective to a constitutional democratic approach since the end of the last century. This turn has not been immediate but has slowly followed the move from economic to constitutional values of the Union,
[1] as well as a rampant digital environment which, in the first decade of this century, started to be populated by new private entities gaining areas of powers by processing data and information in a liberal constitutional environment. 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 contributed to the rise of the constitutional dimension of the Union. The interferences of algorithmic technologies with fundamental rights and the rise of private powers online have triggered a European constitutional reaction towards a new phase of modern constitutionalism, namely digital constitutionalism.

This process can be framed within the challenges raised by globalisation questioning the traditional role of constitutional democracies.[2] Together with other transnational phenomena, the Internet has played a pivotal role in providing new opportunities to exercise fundamental rights and freedoms,[3] while putting democratic constitutional state under pressure not only in terms of the territorial application of sovereign powers but also with regard to the balancing between innovation and the protection of constitutional values. In order to face these challenges, the Union adopted a liberal approach to the digital environment at the end of the last century. This political choice has encouraged the private sector to exploit the opportunities deriving from the use of a low-cost global communication technology for developing new business models without any physical burden and regardless of their location. Precisely, the process of platformisation of the

[1] Giuliano Amato and Elena Paciotti (eds), *Verso l'Europa dei diritti. Lo Spazio europeo di liberta, sicurezza e giustizia* (Il Mulino 2005); Cesare Pinelli, *Il momento della scrittura. Contributo al dibattito sulla Costituzione europea* (Il Mulino 2002); Alessandro Pizzorusso, *Il patrimonio costituzionale europeo* (Il Mulino 2002).
[2] Mark Tushnet, 'The Inevitable Globalization of Constitutional Law' (2009) 49 Virginia Journal of International Law 985.
[3] Jack M. Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 New York University Law Review 1.

digital environment,[4] where platforms with different business models and activities like Facebook,[5] have been considered as neutral service providers rather than active providers. They do not usually produce or create content but instead host and organise information and data for profit. At first glance, platforms would just provide digital spaces where users share their views or access services.

Nonetheless, the development of new algorithmic technologies to profile users and organise content has led these actors to exercise a more pervasive control over information and data. These technologies indeed play a critical role to create targeted services attracting more customers while providing precise windows of visibility and engagement for businesses and organisation to advertise their products and services. To achieve this business purpose, the collection and organisation of vast amounts of data and content become a constitutive activity. Algorithmic technologies provide the possibility to process huge amounts of information,[6] with the result that online platforms can access and profile almost everything about individuals and their lives, as the Cambridge Analytica scandal has shown.[7] The business logics driven by profit maximisation has frustrated the flourishing framework of freedoms promised by the Internet. The processing of information and data has entrusted these actors with almost exclusive control over online content, transforming their role into something more than a mere intermediary. The emergence of new private entities in the information society has led to a paradigmatic shift of power in the algorithmic society.[8]

The US technological optimism in the aftermath of the Internet has then transformed to a form of European constitutional caution before the rise by of transnational actors performing functions traditionally vested in public authorities. The private development of digital and automated technologies has not only, on the one hand, challenged the protection of individuals' fundamental rights such as freedom of expression and data protection. Even more importantly, on the other hand, this new technological framework has also empowered transnational corporations operating in the digital environment to perform quasi-public functions in the transnational context.

Within this framework, this chapter analyses the path leading the Union to adopt a constitutional approach concerning the digital environment in the last thirty years. It aims to explain the reasons for a paradigmatic shift from a liberal to a constitutional democratic approach. This chapter focuses on three phases: digital liberalism, judicial activism and digital constitutionalism. For each phase, the chapter addresses the evolution of the regulation of online content and data, as influenced by the role of the Council of Europe. The first part of this chapter

[4] Anne Helmond, 'The Platformization of the Web: Making Web Data Platform Ready' (2015) 1(2) Social Media + Society 1.

[5] Geoffrey G. Parker, Marshall W. Van Alstyne and Sangett P. Choudary, *Platform Revolution – How Networked Markets are Transforming the Economy – And How to Make them Work for You* (WW Norton & Company Inc 2017); Nick Srnicek, 'The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model' (2017) 23(4) Juncture 254.

[6] Solon Barocas, Sophie Hood and Malte Ziewitz, 'Governing Algorithms: A Provocation Piece' (2013) <https://ssrn.com/abstract=2245322> accessed 20 June 2018; Caryn Devins and others, 'The Law and Big Data' (2017) 27 Cornell Journal of Law and Public Policy 357; Tarleton Gillespie, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (eds) *Media Technologies Essays on Communication, Materiality, and Society* 167 (Oxford University Press 2014).

[7] Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper Collins 2019).

[8] Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 University of California Davis 1151.

focuses on framing the first steps taken by the Union in the phase of digital liberalism at the end of the last century. The second part analyses the role of judicial activism in moving the attention from fundamental freedoms to fundamental rights online in the aftermath of the adoption of the Lisbon Treaty. The third part focuses on the phase of digital constitutionalism and the shift in the approach of the Union from digital liberalism to a constitutional democratic strategy.

2. The First Phase: Digital Liberalism

The signing of the Treaty of Rome in 1957 set the primary goal of the European Economic Community: the establishment of a common market and the approximation of economic policies among Member States.[9] At that time, digital technologies were far from demonstrating their potentialities. The founding fathers could not foresee how the digital revolution would have provided new possibilities for economic growth while introducing a new layer of complexity for the regulation of the internal market. Until the adoption of Charter in 2000 and the recognition of its binding effects in 2009,[10] the Union approach was firmly based on this liberal imprinting based on economic pillars, namely the fundamental freedoms. Even if not exclusively, the free movement of persons, the freedom of establishment, the freedom to provide goods and services and the free movement of capital can (still) be considered the primary drivers of European integration and the growth of the internal market.[11] The goal of this system was to 'to protect society and create an equitable Internet environment'.[12] Therefore, the consolidation and harmonisation of the single market was one of the primary drivers of the Union approach at the end of the last century.

This liberal framework was transposed in the regulation of the digital environment. In the field of data and content, Directive 95/46/EC ('Data Protection Directive') and Directive 2000/31/EC ('e-Commerce Directive') show such a liberal frame oriented to ensure the smooth development of the internal market.[13] Precisely, online intermediaries have been exempted from liability for transmitting or hosting unlawful third-party content while the processing of personal data was harmonised to promote the free circulation of personal data in the internal market. In other words, in the lack of a European constitutional framework at that time, the economic imprinting of the internal market has characterised the first approach of the Union in the field of new digital technologies, namely digital liberalism.

Such a liberal approach does not only reflect the economic imprinting of the Union but also it can be framed within the debate about Internet regulation at the end of the last century. An extensive technological optimism welcomed the advent of the Internet at the end of the last

[9] Kamiel Mortelmans, 'The Common Market, the Internal Market and the Single Market, What's in a Market?' (1998) 35(1) Common Market Law Review 101.
[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] Matthew Feeley, 'EU Internet Regulation Policy: The Rise of Self-Regulation' (1999) 22(1) Boston College International and Comparative Law Review 159, 167.
[13] 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.

century from the western side of the Atlantic. As we will be explained in Chapter III, in the aftermath of the Internet, the digital environment was considered an area where public actors cannot interfere. Barlow stated that the digital space is a new world separate from the atomic one, where 'legal concepts of property, expression, identity, movement, and context do not apply'.[14] As for all new undiscovered world, cyberspace was considered as an opportunity: a dreaming land where social behaviours were not exposed to tyrannical constraints. In other words, cyberspace was considered as a new world completely separate from the atomic reality, thus, blocking the exercise of the traditional power by governments and lawmakers. Johnson and Post also supported the independent nature of the digital environment.[15] Both 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.[16] Stated differently, these liberal ideas are based on a bottom-up approach: rather than relying on traditional public law-making power to set the norms regulating the digital environment, digital communities would be capable of participating and creating the rules governing their online spaces. This is also because the characteristics of the digital environment would oblige governments and lawmakers to adopt a free-market regulation. It is not by chance if Froomkin defines the Internet as the 'Modern Hydra'.[17] No matter what the effort is to cut the heads of the mythical beast, others will grow up. Therefore, any top-down attempt of regulating the online environment (cutting one of the Hydra's heads) would fail since communities would easily react against such interferences (the growth of new heads).

This metaphor does not only highlight the liberal narrative and challenges that governments face when trying to strike a fair balance between innovation and protection of constitutional rights. Even more importantly, this framework also shows some of the reasons why democratic constitutional states have adopted a free-market approach when dealing with the digital environment.[18] At the end of the last century, the adoption of a paternalistic approach could hinder the development of new digital services. A strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were poised to revolutionise the entire society. Besides, the rise of digital capitalism, or surveillance capitalism, was highly convenient not only for ensuring paths of economy growth or fostering economic fundamental freedoms but also for the exercise of public powers.[19] The liberal approach adopted in the aftermath of the Internet is also the result of an invisible handshake based on neoliberal understanding where Governments have refrained to regulate private companies operating in the

[14] Ibid.
[15] David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367, 1371.
[16] David R. Johnson and David Post, 'And How Shall the Net be Governed?' in Brian Kahin and James Keller (eds) *Coordinating the Internet* 62 (MIT Press 1997).
[17] A. Michael Froomkin, 'The Internet as a Source of Regulatory Arbitrage' in Brian Kahin and Charles Nesson (eds), *Borders in Cyberspace* 129 (MIT Press 1997).
[18] 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' (2011) 76 GeoJournal 1; Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64(3) Emory Law Journal 677.
[19] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Polity Press 2019).

online environment to benefit from the unaccountable cooperation with the private sector.[20] The lack of transparency and accountability made easier for public actors to rely on data for security and surveillance purposes, thus, formally escaping constitutional safeguards.

Within this framework, a migration of constitutional ideas has occurred across the Atlantic. As underlined by Christou and Simpson, the US vision of the Internet as a self-regulatory environment driven by neoliberal globalisation theories has influenced the Union's legal framework even if the Union has always shown its intention to a cooperative approach to the regulation of the Internet.[21] This difference is not casual but, as underlined in Chapter I, it is the result of different constitutional premises across the Atlantic. Nonetheless, at the end of the last century, the first phase of digital liberalism was predominant because new digital technologies were considered as an opportunity to grow and prosper when they did not represent a potential threat to individuals' constitutional rights and freedoms. The Union's approach was more concerned about the potential impacts of regulatory burdens on economic (fundamental) freedoms and innovation rather than on the protection of individuals' rights and freedoms which, instead, a public intervention in the digital environment would have undermined. 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 public powers. The following sections analyse how the phase of digital liberalism examining the Union's regulatory path at the beginning of this century in the field of content and data.

2.1 Exempting Online Intermediaries from Liability

The e-Commerce Directive can provide interesting clues to understand the European liberal approach to the digital environment. The reading of the first Recitals can unveil that the primary aim of the Union was 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'. [22] As also observed by the Economic and Social Committee before the adoption of the e-Commerce Directive, 'to bring the possible benefits fully to bear, it is necessary both to eliminate legal constraints on electronic commerce and to create conditions whereby potential users of electronic commercial services (both consumers and businesses) can have confidence in e-commerce. An optimum balance must be found between these two requirements. Given the wide scope of the directive under review and its complex interrelationship with other areas of regulation, a very careful and responsible approach will be needed'.[23]

[20] Michael Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8(2) Virginia Journal of Law & Technology 1.
[21] George Christou, and Seamus Simpson, 'The Internet and Public–Private Governance in the European Union' (2006) 26(1) Journal of Public Policy 43. See also Edward Halpin and Seamus Simpson, 'Between Self-Regulation and Intervention in the Networked Economy: The European Union and Internet Policy' (2002) 28(4) Journal of Information Science 285.
[22] E-Commerce Directive (n 13), Recitals 1-3.
[23] Opinion of the Economic and Social Committee on the 'Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market' (1999) C 169, 36–42.

To achieve this purpose, the e-Commerce Directive exempts from liability Internet service providers (or online intermediaries) for the unlawful conducts of third parties.[24] Among online intermediaries,[25] 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 (i.e. notice and takedown).[26]

This European system was not a novelty but reflected the US approach to online intermediaries. Back at the end of the last century, the US Congress enacted the Communication Decency Act,[27] and the Digital Millennium Copyright Act.[28] By recognising the non-involvement of online intermediaries in the creation of content, both these measures exempts in different ways online intermediaries from liability for transmitting or hosting unlawful third-party content.[29] When the US Congress passed Section 230 of the Communication Decency Act, the primary aim was to encourage free expression and development of the digital environment. In order to achieve this objective, the choice was to exempt computer services from liability for third-party conducts.[30] Otherwise, online intermediaries would have been subject to a broad and unpredictable range of cases concerning their liability for editing third-party content since their activities consisted on transmitting and hosting vast amount of content.[31] Since, in the lack of any legal shield, this situation would have negatively affected the development of new digital services in the aftermath of the Internet, the US policy aimed to encourage online intermediaries to grow

[24] Maria L. Montagnani, *Internet, contenuti illeciti e responsabilita degli intermediari* (Egea 2018); Graeme B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2017); Marco Bassini, 'La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità 'complessa'?' (2015) Federalismi.it <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=30349> accessed 12 June 2020; Oreste Pollicino and Ernesto Apa, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective* (Egea 2013); Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law Review 1455; Marcello De Cata, *La responsabilita civile dell'*internet service provider (Giuffrè 2010); Lilian Edwards, 'The Problem of Intermediary Service Provider Liability' in Lilian Edwards (ed.), *The New Legal Framework for E-Commerce in Europe* 93 (Hart 2005); Emilio Tosi and Vincenzo Franceschelli, *Le regole giuridiche del commercio elettronico* (Giuffrè 2003); Giovanni M. Riccio, *La responsabilita degli internet providers* (Giappichelli 2002); Salvatore Sica e Pasquale Stanzione, *Commercio elettronico e categorie civilistiche* (Giuffrè 2002).

[25] This ban applies to three categories of online intermediaries: access providers, caching providers and hosting providers E-Commerce Directive, (n 13), Arts 12-14.

[26] Ibid, Art 14. Nonetheless, Member States have implemented this rule in different ways like Italy. See Marco Bassini, 'Mambo Italiano: the Italian perilous way on ISP liability' in Tuomas Ojanen and Byliana Petkova (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (forthcoming, Edward Elgar); Giuseppe Cassano and Iacopo P. Cimino, 'Il nuovo regime di responsabilita dei providers: verso la creazione di un novello "censore telematico"? Un primo commento agli artt. 14 -17 del d.lgs. 70/2003' (2004) (3) Giurisprudenza italiana 671; Francecsco Delfini, 'La responsabilita dei prestatori intermediari nella direttiva 2000/13/CE e nel d.lgs. 70/2003' (2004) (1) Rivista di diritto privato 55.

[27] Communication Decency Act, 47 U.S.C., Section 230

[28] Digital Millennium Copyright Act, 17 U.S.C., Section 512.

[29] Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017).

[30] Rosario Petruso, *Le responsabilita degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto* (Giappichelli 2019).

[31] 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).

and develop their business under the protection of the safe harbour and the Good Samaritan rule.[32] It is not by chance that Section 230 has been described as 'the twenty-six words that created the Internet'.[33] This provision has opened the door towards the evolution of the digital environment and still constitute the basic pillar legitimising online platforms' activities,[34] showing the primacy of the First Amendment in US constitutionalism.[35]

The US model has influenced the political choice on the eastern side of the Atlantic. The aim of the European liability exemption is twofold. Firstly, the e-Commerce Directive focuses on fostering the free movement of information society services as a 'reflection in Community law of a more general principle, namely freedom of expression',[36] as enshrined at that time only by Article 10(1) of the Convention.[37] Here, it is worth observing how the right to freedom of expression was strictly connected to the rise of new digital services and, therefore, their development was functional to this purpose. In other words, according to the Union approach, these new technologies would constitute a positive driver for promoting this fundamental right in the internal market. Secondly, the exemption of liability aims to avoid holding liable entities that do not have effective control over the content transmitted or hosted since they perform activities merely neutral, automatic and passive.[38] In order to achieve this purpose, the e-Commerce Directive does not only exempt online intermediaries from liability but also sets forth a general rule banning general monitoring.[39] 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.[40] Even in this case, this rule aims to avoid that online intermediaries would be overwhelmed by legal obligations which would require additional financial and human resources, *de facto*, making their activities not profitable due to the vast amount of content they transmit or host.

Therefore, online intermediaries have been generally considered neither accountable nor responsible (i.e. safe harbour) since platforms are not aware (or in control) of illegal content transmitted or hosted. This legal framework is reasonable as long as online intermediaries only performed passive activities, such as providing access or space to host third-party content. However, the evolving framework of e-commerce marketplace, search engines and social networks organizing and moderating content through artificial intelligence technologies has firmly challenged the legal exemption of liability which is formally based on the lack of awareness and control over third-party content. If, on the one hand, the choice to exempt online

[32] Zeran v. Am. Online, Inc. 129 F.3d 327, 330 (4th Cir. 1997).
[33] Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).
[34] Danielle K. Citron and Benjamin Wittes, 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity' (2017) 86 Fordham Law Review 401; Jeff Kosseff, 'Defending Section 230: The Value of Intermediary Immunity' (2010) 15 Journal of Technology Law & Policy 123; Jack M. Balkin, 'The Future of Free Expression in a Digital Age' (2009) 36 Pepperdine Law Review, 427.
[35] Alexander Meiklejohn, 'The First Amendment is an Absolute' (1961) The Supreme Court Review 245.
[36] E-Commerce Directive (n 13), Recital 9.
[37] European Convention on Human Rights (1950).
[38] E-Commerce Directive (n 13), Recital 42.
[39] Ibid, Art 15.
[40] 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. Ibid, Art 15(2).

intermediaries from liability was aimed to foster the development of new digital services, thus, contributing to the internal market, on the other hand, such a liberal approach has led to the rise and consolidation of new business actors in the internal market.

Furthermore, by imposing upon hosting providers the obligation to remove online content based on their awareness or control, this system of liability has entrusted online platforms with the power to autonomously decide whether to remove or block vast amounts of content to mitigate the risk to be held liable. Since these actors are private and there is no requirement that public authorities assess the lawfulness of online content before removal or blocking, online platforms would likely apply a risk-based approach to avoid financial burdens from their failure to comply with their duty to remove or block (i.e. collateral censorship).[41] This liability regime incentivises online platforms to focus on minimising this economic risk rather than adopting a fundamental rights-based approach. Besides, as we will examine in Chapter V, this system leaves platforms free to organise content based on the logic of moderation driven by profit maximisation. This system of liability works as a legal shield for online platforms,[42] and, even more importantly, encourages them to set their rules to organise and moderate content based on private interests and other discretionary (but opaque) conditions.[43] This incentive to organise and moderate content for commercial purposes can be considered one of the primary reasons explaining how online platforms enjoy a broad margin in determining the scope of protection of fundamental rights in the digital environment. As the next subsection shows, even the Union's approach to personal data has favoured the rise of private powers online.

2.2 Ensuring the Free Circulation of Personal Data

When focusing on the field of data, at first glance, it could be observed that the Union has not adopted a liberal approach. Unlike in the case of content, rather than exempting online intermediaries from liability, the Union introduced obligations concerning 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.[44]

The rise data protection law has been a positive answer to the new challenges of the information society where public and private entities implemented new systems to process data and interfere with the right to privacy. In other words, if the right to privacy was conceived to meet the interests of individuals' protection during the last century,[45] the information society has shown how the right to privacy could not be enough to protect individuals against interferences coming from the increasing processing of personal data. Therefore, this situation has led to the rise of a positive approach to increase the degree of transparency and accountability in the field

[41] Regarding the risk of collateral censorship, see Delfi AS v Estonia (2015); MTE v Hungary (2016). See Jack M. Balkin, 'Old-School/New-School Speech Regulation' (2014) 128 Harvard Law Review 2296; Felix T. Wu, 'Collateral Censorship and the Limits of Intermediary Immunity' (2011) 87(1) Notre Dame Law Review 293.

[42] Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487; Rebecca Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment' (2008) 76 George Washington Law Review 986.

[43] Danielle Keats Citron and Helen L. Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age' (2011) 91 Boston University Law Review 1436.

[44] Data Protection Directive (n 13), Recital 4.

[45] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

of data.[46] This process can be examined looking at the consolidation of the constitutional dimension of the right to protection of personal data in the framework of the Council of Europe. Together with the role of ECHR the Strasbourg Court, the Convention No. 108 has been the first instrument to deal with the protection of individuals with regard to automatic processing of personal data in 1981.[47] The concerns relating to automated processing were already underlined when artificial intelligence technologies were not still spread. Nonetheless, ensuring the protection of personal data taking account the increasing flow of information across frontiers was the first aim of this convention which was modernised in 2018.[48]

When focusing on the Union, at first glance, the Data Protection Directive could fit within this framework of safeguards and guarantees. In 1995, the adoption of the Data Protection Directive would suggest a constitutional reaction against the challenges raised by the information society, as also highlighted by the Council of Europe. A closer look can reveal how the Union policy was instead oriented to encourage the free movement of data as a way to promote the growth of the internal market. The Data Protection Directive highlighted 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.[49] Although the processing of personal data shall serve mankind and aim to protect the privacy of data subjects,[50] the economic-centric frame of the European approach with regard to the protection of personal data cannot be disregarded.

The liberal approach of the Union in the field of data is counterintuitive. The purposes of the internal market approach have led to the adoption of the Data Protection Directive. This was also the mandatory path at that time since, in 1995, the lack of a European constitutional framework protecting privacy and data protection was a limit to the constitutional scope of the Data Protection Directive which indeed finds its roots in the internal market clause.[51] The liberal imprinting and functional approach of data protection can be understood by focusing on the first proposal of the Commission in 1990.[52] According to the Commission, 'a Community approach towards the protection of individuals in relation to the processing of personal data is also essential to the development of the data processing industry and of value-added data communication services'.[53]

In the years after the adoption of the Data Protection Directive, the Union has not made steps forward to modernise data protection rules to address the new challenges raised by transnational private actors such as users' profiling. The time of adoption together with the lack of any

[46] Serge Gutwirth and Paul de Hert, 'Regulating Profiling in a Democratic Constitutional States' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* 271 (Springer 2006).
[47] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).
[48] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018).
[49] Data Protection Directive (n 13), Recital 3.
[50] Ibid*,* Recital 2.
[51] Laima Jančiūtė, 'EU Data Protection and "Treaty-base Games": When Fundamental Rights are Wearing Market-making Clothes' in Ronald Leenes and others (eds), *Data Protection and Privacy. The Age of Intelligent Machine* (Hart 2017).
[52] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (1990) COM(90) 314 final.
[53] Ibid, 4.

amendment in more than twenty years could explain why European data protection law has failed to face the challenges raised by online platforms in the digital environment. At the end of the last century, the Union was more concerned to ensure a common legal framework to promote the circulation of data. However, at the same time, it could not foresee how the digital environment would have affected the right to privacy and data protection. In 1995, 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. Although it was reasonable not to foresee these challenges, the first draft of reviewing the privacy and data protection regime has been proposed only in 2012,[54] and the GDPR entered into force in 2016, even without any binding effect until May 2018.[55] In other words, the (digital) liberal approach of the Union in this field is also the result of an omissive approach rather than a political choice like in the field of content.

Beyond these diachronic reasons, the characteristics of European directives can also underline the inadequacy of the European data protection law to face transnational digital challenges. Unlike regulations which are directly applicable once they entry into force without the need for domestic implementation, the norms provided by European directives outline just the result that Member States should achieve and are not generally applicable without domestic implementation. Therefore, minimum harmonisation should have provided a common legal framework for promoting the free circulation of personal data in the Union. The Data Protection Directive left Member States' free to exercise their margins of discretion when implementing data protection rules within their domestic legal order. Therefore, despite the possibility to rely on harmonised framework in the Union, the Data Protection Directive could not ensure that degree of uniformity able to address transnational challenges. Even if these considerations could also be extended to the e-Commerce Directive, in that case, the Union has introduced new legal instruments to tackle illicit content.[56] Whereas, in the framework of data, several Member States have already adopted their national laws on data protection before the adoption of the Data Protection Directive. These laws were already rooted in the legal tradition of each Member States as the two models of France and Germany show.[57] Therefore, 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 the challenges raised by online platforms.

Within this framework, the fragmentation of domestic regimes and the lack of any revision at supranational level have been the primary drivers encouraging the turning of freedoms into

[54] 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.
[55] 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.
[56] See, e.g., Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society (2001) OJ L 167/10; Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (2008) OJ L 328/55.
[57] Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés; Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) of 27 January 1977.

powers based on the processing of vast amounts of (personal) data on a global scale. In other words, in the field of data, the rise and consolidation of new actors in the digital environment have been the result of a liberal frame made of regulatory design and omission. Like in the field of content, this liberal approach has led to the shift from freedoms to power, thus, encouraging the Union to adopt a (digital) constitutional strategy.

3. The Second Phase: Judicial Activism

The rampant evolution of the digital environment has put under pressure the liberal imprinting of the Union at the beginning of this century. At the very least, two events have led to the end of the first (liberal) season leading to a new phase of the European constitutional path characterised by the role of the ECJ in framing fundamental rights in the digital environment. The first event triggering this phase of judicial activism concerned the rise and consolidation of new private actors online, whereas the second concerns the Charter as a bill of rights of the Union in the aftermath of the Lisbon Treaty.[58]

Firstly, at the end of the last century, online intermediaries just provide access, transmit, and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties like hosting. In other words, online intermediaries were mere service providers or data processor without being involved in the organisation or moderation of content or the determination of data processing purposes. When focusing on the role that some hosting providers, such as social media platforms and search engines, have been actively playing since approximately the first decade of 2000, these considerations hardly apply. Since the end of the last century, indeed, the Internet has changed its face. From a channel to transmit and host information published on webpages made just of text and small pictures, it has started to become an environment where offering products and services and allow people to communicate cross border and exchange information and data, primarily through online platforms.[59] In other words, from a mere channel of communication and hosting, the Internet became a social layer. Within this framework, new business models have started to emerge by benefiting of the characteristics of this global channel of communication and, even, public actors exploited this new channel for monitoring and surveillance purposes.[60]

Unlike traditional access or hosting providers, the primary activities of online platforms do not consist of providing free online spaces where users can share information and opinions. On the contrary, these actors gain profits from the processing and analysis of information and data which attract different forms of revenues like advertising or allow them to increasingly attract

[58] Grainne De Burca, 'The Road Not Taken: The EU as a Global Human Rights Actor' (2011) 105(4) American Journal of International Law 649; Sionhaid Douglas-Scott, 'The European Union and Human Rights after the Treaty of Lisbon' (2011) 11(4) Human Rights Law Review 645; Alessandro Pace, 'A che serve la Carta dei diritti fondamentali dell'Unione europea? Appunti preliminari' (2011) (1) Giurisprudenza costituzionale 193; Roberto Mastroianni, 'I diritti fondamentali dopo Lisbona tra conferme europee e malintesi nazionali' (2010) (4) Diritto Pubblico Comparato ed Europeo XXI; Marta Cartabia, 'I diritti fondamentali in Europa dopo Lisbona. Verso nuovi equilibri?' (2010) (3) Giornale di diritto amministrativo 221; Marta Cartabia, 'Europe and Rights: Taking Dialogue Seriously' (2009) 5(1) European Constitutional Law Review 5; Sionhaid Douglas-Scott, 'A Tale of Two Courts: Luxembourg, Strasbourg and the Growing European Human Rights Acquis' (2006) 43 Common Market Law Review 629.

[59] Nick Srnicek, *Platform Capitalism* (Polity Press 2016).

[60] David Lyon, *Surveillance After Snowden* (Polity Press 2015).

new customers of their products and services.[61] In the case of social media, in order to avoid the escape of users' which provide the information on which online platforms' profits are based, these actors need to firmly govern their digital spaces by implementing automated decision-making technologies to moderate online content and process data.[62] These systems help online platforms to attract revenues from users' profiling by ensuring a healthy and efficient online community, thus, contributing to protect the corporate image and show commitments with ethic values. The increasing involvement of online platforms in the organisation of content and the profiling of users' preferences by using artificial intelligence technologies has transformed their role 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 for business purposes has led these entities to perform organisational 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 with the adoption of the Lisbon Treaty can be considered the other primary driver pushing European digital constitutionalism towards a new phase. This step has contributed to codifying the constitutional dimension of the European (digital) environment.[63] 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.[64] 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.[65] Nevertheless, although the Union made reference to the framework of the Convention as explicitly mentioned in the Recitals of the e-Commerce Directive and the Data Protection Directive, the lack of accession of the Union to the Convention system has always limited the scope of this acknowledgement,[66] thus, leaving Member States to take into account the safeguards of the Convention within their domestic system.

Also for this reason, the Lisbon Treaty has constituted a crucial step allowing the right to freedom of expression,[67] private and family life,[68] and the protection of personal data,[69] as already enshrined in the Charter, to become binding vis-a-via Member States and European institutions,[70] which can interfere with these rights only according to the conditions established by the

[61] Martin Moore and Damian Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).
[62] Tarleton Gillespie, *Custodians of The Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).
[63] Consolidated version of Treaty on the European Union (2012) OJ C 326/13, Art 6(1).
[64] Convention (n 37) Arts 8, 10.
[65] 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' (2019) 25 European Law Journal 155.
[66] Bruno De Witte and Sejla Imanovic, 'Opinion 2/13 on Accession to the ECHR: Defending the EU Legal Order against a Foreign Human Rights Court' (2015) 5 European Law Review 683 Paul Craig, 'EU Accession to the ECHR: Competence, Procedure and Substance' (2013) 35 Fordham International Law Journal 111; Sionhaid Douglas-Scott, 'The Relationship between the EU and the ECHR Five Years on from the Treaty of Lisbon' in Sybe De Vries, Ulf Bernitz and Stephen Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing* 41 (Hart 2015).
[67] Charter (n 63), Art 11(1).
[68] Ibid, Art 7.
[69] Ibid, Art 8(1).
[70] Ibid, Art 51.

Charter.[71] Besides, similarly to the Convention,[72] the Charter adds another important piece of the European constitutional puzzle by prohibiting the abuse of rights consisting of the 'destruction of any of the rights and freedoms recognised in this Charter or at their limitation to a greater extent than is provided for herein'.[73] This approach to constitutionalism can be considered reverse with respect to Member States since the constitutional protection of fundamental rights at the European level comes from the evolution of the economic identity.

Within this new constitutional framework characterised by the European legislative inertia before the new challenges of the information society, the ECJ started to act as quasi-constitutional court.[74] The court applied the Charter as a parameter to assess the validity and interpret European legal instruments, thus, moving from a formal dimension to a substantial application of fundamental rights (i.e. constitutional law in action). Nevertheless, it is worth observing that this process started even before the Maastricht Treaty entered into force when the fundamental rights started to be applied as limitations for fundamental freedom and common market principles.[75] Precisely, the recognition of fundamental rights as general principles of EU law has opened the door towards a balancing exercise between fundamentals freedoms and rights, or between the economic and constitutional dimension of the Union.[76]

Therefore, the Charter has raised as a tool for judicial power to answer new digital challenges in the lack of any approach from political power. As the next subsections show, the ECJ has adopted a teleological approach focusing on the need to ensure the effective protection of these constitutional interests to cope with the threats coming from new technologies implemented by public actors and private business such as online platforms. 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 to highlight the challenges for fundamental rights online, thus, promoting the transition from a mere economic perspective to a new constitutional phase characterising European digital constitutionalism.

3.1 From Economic Interests to Fundamental Rights

In the field of content, the ECJ's judicial activism has contributed to unveiling the constitutional dimension of online platforms' liability. Apart from a narrow reference to Article 10 of the Convention, the e-Commerce Directive does not clarify the relationship between individuals' fundamental rights, primarily freedom of expression, and the freedom to conduct business of

[71] Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2013) 8(3) European Constitutional Law Review 375.
[72] Convention (n 37), Art 17.
[73] Charter (n 63), Art 54.
[74] Grainne De Burca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20(2) Maastricht Journal of European and Comparative Law 168.
[75] See Case C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich (2003) ECR I-905; Case C-36/02, Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn (2004) ECR I-9609; Case C-341/05, Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet (2007) ECR I-11767; Case C-438/05, Viking Line ABP v The International transport Workers' Federation, the Finnish Seaman's Union (2007) ECR I-10779.
[76] See Case 29/69, Erich Stauder v City of Ulm - Sozialamt (1969); Case 11/70, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel (1970); Case 4/73, J. Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft (1977).

online intermediaries. Even before the adoption of the Lisbon Treaty, the ECJ focused on the boundaries of online intermediaries' liability regime in two landmark decisions.

In *Google France,*[77] the ECJ underlined 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 original liberal frame characterising 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'.[78] Likewise, although the ECJ recognised that Google established 'the order of display according to, inter alia, the remuneration paid by the advertisers',[79] this situation does not deprive the search engine from the exemption of liability established by the e-Commerce Directive.[80] Although neither the Advocate General nor the ECJ did recognise the active role of this provider, this judicial economic and the role of automated processing systems had already shown their relevance in shaping the field of online content.

The ECJ made a step forward in *L'Oréal*.[81] In this case, the offering of assistance, including the optimisation, presentation or promotion of the offers for sale, was not considered a neutral activity performed by the provider.[82] It is worth observing how, firstly, the court did not recall the opinion of Poiares Maduro in *Google France*, thus, limiting the scope of the economic interests of online platforms in providing their services. Secondly, its decision acknowledged how automated technologies have led some providers to perform an active role rather than the mere passive provisions of digital products and services.

Nevertheless, both decisions still show a prevalent economic judicial frame in the field of content. This approach is also the result of the lack of a constitutional parameter to apply at the European level to address the degree of liability of these actors. It is not by chance whether, in 2011 after the adoption of the Lisbon Treaty, the ECJ shifted this approach from a merely economic perspective to a fundamental rights-based approach. In 2011, without amending the legal framework of the e-Commerce Directive, the Commission aimed to ensure a harmonised framework for 'notice-and-action' procedures.[83] This is because online intermediaries were

[77] 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-2417.
[78] Opinion of Advocate General in 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 (22 September 2009), 144
[79] Cases C-236/08, C-237/08 and C-238/08 (n 77), 115.
[80] Ibid, 116.
[81] Case 324/09, L'Oréal SA and Others v. eBay International AG and Others (2011) ECR I-06011.
[82] Ibid, 116.
[83] Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions, A Coherent Framework for Building Trust in the Digital Single Market for E-Commerce and Online Services COM(2011) 942 final.

facing legal uncertainty due to the fragmentation of European rules on this process. Even if the framework was focused on improving legal certainty on the market based on a self-regulatory strategy and the maintenance of the system of liability introduced by the e-Commerce Directive, nonetheless, the Union started to focus on the need to tackle illegal content online, ensure transparent procedures which can provide a proportionate framework to protect fundamental rights.[84]

The adoption of a constitutional interpretative angle is clear when addressing two cases involving online intermediaries and, primarily, the extent of the ban on general monitoring.[85] In *Scarlet* and *Netlog*,[86] the question of the domestic court aimed to understand whether Member States could allow national courts to order online platforms to set filtering systems of all electronic communications for preventing the dissemination of illicit online content. The e-Commerce Directive prohibits Member States from imposing either a general obligation on providers to monitor the information that they transmit or store or a general obligation to actively seek facts or circumstances indicating illegal activity. Therefore, the primary question of the national court concerned the proportionality of such an injunction, thus, leading the ECJ to interpret the protection of fundamental rights in the Charter. The ECJ dealt with the complex topic of finding a balance between the need to tackle illegal content and users' fundamental rights, precisely the right to privacy and freedom of expression as well as the interests of the platforms not to be overwhelmed by expensive monitoring systems. According to the ECJ, an injunction to install a general filtering system would have not respected the freedom to conduct business of online intermediaries.[87] 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.[88] As a result, 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.

From that moment, the ECJ has relied on the Charter to assess the framework of the e-Commerce Directive. For instance, in *Telekabel* and *Mc Fadden*,[89] the ECJ addressed two similar 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 European fundamental rights. The ECJ upheld the

[84] Aleksandra Kuczerawy, 'Intermediary liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31(1) Computer Law & Security Review 46.
[85] Martin Husovec, *Injunctions Against Intermediaries in the European Union* (Cambridge University Press 2017).
[86] Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (2011) ECR I-11959; Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (2012). See Stefan Kulk & Frederik Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34(11) European Intellectual Property Review 791.
[87] Case C-70/10 (n 86), 50.
[88] Charter (n 61), Arts 8, 11.
[89] Case C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (2014); Case C-484/14, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (2016). See Martin Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (2017) 12(2) Journal of Intellectual Property Law and Practice 115.

interpretation of the referring national court on the same (constitutional) basis argued in *Scarlet* and *Netlog,* by concluding that the fundamental rights recognised by European law have to be interpreted as not precluding a court injunction such as that of the case in question. This constitutional interpretation has led the ECJ to extend constitutional safeguard to the digital environment underlining how the economic frame could not be considered enough to address new digital challenges. Even more recently, as we will examine in Chapter V, the ECJ has interpreted the framework of the e-Commerce Directive in *Eva Glawischnig-Piesczek* to interpret the safeguards in the removal of identical and equivalent content.[90]

The Strasbourg Court has also underlined how online intermediaries' activities involve fundamental right. Although the court does not rely on the e-Commerce Directive as a parameter, it has repeatedly addressed cases involving the responsibility of online intermediaries for hosting unlawful content such as defamatory comments.[91] Precisely, the court has highlighted the potential chilling effect on freedom of expression online resulting from holding platforms' liable in relation to third-partied conducts.[92]

Despite these judicial efforts, the challenges raised by online platforms looked far from being solved, primarily, when focusing on the liability for actively organizing third-party content as well as transparency and accountability when autonomously implementing automated decision-making technologies for moderating content. These systems allow platforms to perform their activities in a manner that questions not only the liability system of the e-Commerce Directive but also constitutional values online such as the protection of fundamental rights and the rule of law. As we will examine in Chapter III, since online platforms contribute to defining the standard of protection of rights online on a global scale, the ECJ has played a crucial role in defining the role of constitutional values in the information society. Therefore, highlighting the role for fundamental rights online have been an important step forward in the evolution of European digital constitutionalism. As the next sections show, the Union is going even further in the field of content by orienting its approach not only on reviewing online platforms' liability but also towards the regulation of content moderation through the introduction of transparency and accountability safeguards.

3.2 The Judicial Path towards Digital Privacy

The field of content has already revealed the role of the ECJ in addressing the new constitutional challenges of the information society. This judicial approach has not only focused on underlining the relevance of fundamental rights' protection in relation to online content but also consolidating and emancipating the right to data protection in the European framework.[93] Both the recognition of the Charter as a primary source of EU law and the increasing relevance of data in the

[90] Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited (2019).
[91] See Delfi AS v. Estonia, Judgement (2015); Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v. Hungary, Judgement (2016); Rolf Anders Daniel Pihl v. Sweden (2017).
[92] Robert Spano, 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665.
[93] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015); Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* 3 (Springer 2009).

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.[94]

As a first step, in *Lindqvist*,[95] the ECJ highlighted how the objectives of harmonisation of those national rules including the free flow of data between Member States can clash with the safeguarding of the fundamental rights of individuals.[96] Precisely, it underlined how the case in question required to strike a fair balance between conflicting rights, especially the right to freedom of expression and privacy.[97] However, in this case, the judicial focus was still on the right to privacy. Some years later, in the *Promusicae* case,[98] the ECJ has recognised the role of data protection 'namely the right that guarantees protection of personal data and hence of private life',[99] despite its functional link with the protection of privacy.[100]

This scenario changed with the entry into force of the Lisbon Treaty. From that moment, the ECJ has started to apply the Charter to assess the threats for fundamental rights in the information society. Unlike the case of content, the Charter introduced a new fundamental right consisting of the right to protection of personal data.[101] Therefore, in the field of data, the ECJ has not just framed the scope of application of the right to freedom of expression online but it has played a crucial role in the consolidation of this new fundamental right within the European context.

The power of this shift of paradigm has led the ECJ to invalidate Directive 2006/24/EC, [102] due to its disproportionate effects over fundamental rights. In *Digital Rights Ireland*, [103] by assessing, as a constitutional court, the interferences, and potential justifications, with the rights of privacy and data protection established by the Charter, the ECJ has shown to be aware of the risks for the protection of the fundamental rights of European 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'.[104] Moreover, with regard to automated technologies, the ECJ observed that '[t]he need for such

[94] Giusella Finocchiaro, 'La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "Schrems"' (2015) (4-5) Diritto dell'informazione e dell'informatica 779; Oreste Pollicino and Marco Bassini, 'La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo' (2015) (4-5) Diritto dell'informazione e dell'informatica 741.
[95] Case C-101/01, Lindqvist (2003) ECR I-2971.
[96] Ibid, 79-81
[97] Ibid, 86
[98] Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECR I-271 (2008), 63.
[99] Ibid, 63.
[100] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.
[101] Charter (n 61), Art 8.
[102] 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.
[103] 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). See Federico Fabbrini, 'The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal 65.
[104] Cases C-293/12 e C-594/12 (n 103), 56.

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'.[105]

The same constitutional approach can be appreciated in *Schrems,*[106] 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).[107] Even in this case, the ECJ has provided an extensive interpretation of the fundamental right to data protection when reviewing the regime of data transfer established by the Data Protection Directive,[108] in order to ensure 'an adequate level of protection' in the light of 'the protection of the private lives and basic freedoms and rights of individuals'.[109] It is interesting to observe how the ECJ has manipulated the notion of 'adequacy', which, as a result of this new constitutional frame, has moved to a standard of 'equivalence' between the protection afforded to personal data across the Atlantic.[110] 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 'by virtue of Directive 95/46 read in the light of the Charter'.[111] The ECJ adopted the same extensive approach even in the second decision involving the transfer of personal data to the US. As we will examine in Chapter VII, the need to ensure an essentially equivalent level of protection has led the ECJ to invalidate even the adequacy decision called Privacy Shield.[112]

These cases underline the role of the Charter in empowering the ECJ 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 European boundaries. Nevertheless, the case showing the paradigmatic shift from an economic to a constitutional perspective in the field of data is *Google Spain,* for at least two reasons.[113] Firstly, as in *Digital Rights Ireland* and *Schrems,* the ECJ has provided an extensive constitutional interpretation of the right to privacy and data protection to ensure their effective protection. Secondly, unlike the other two cases, the *Google Spain* ruling demonstrates a first judicial attempt to cope with the power of online platforms and answer to the legislative inertia of the Union, thus, laying the foundation of digital constitutionalism.

The way in which ECJ recognised that a search engine like Google falls under the category of 'data controller' show the predominant role privacy and data protection as fundamental rights.

---

[105] Ibid, 55.
[106] Case C-362/14, Maximillian Schrems v Data Protection Commissioner (2015). See Oreste Pollicino and Marco Bassini, 'Bridge Is Down, Data Truck Can't Get Through...A Critical View of the Schrems Judgment in the Context of European Constitutionalism' (2017) 16 Global Community Yearbook of International Law and Jurisprudence 2016 245.
[107] 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.
[108] Data Protection Directive (n 13), Art 25.
[109] Case C-362/14 (n 106), 71.
[110] Ibid, 73.
[111] Ibid.
[112] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (2020).
[113] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014). See Orla Lynskey, 'Control Over Personal Data in A Digital Age: Google Spain V AEPD And Mario Costeja Gonzalez' (2015) 78 Modern Law Review 522; Francesco Pizzetti (eds), *Internet e la tutela della persona: il caso del motore di ricerca* (Passigli Editori 2015).

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'.[114] In other words, considering Google as a mere data processor would have not ensured effective protection to the rights of the data subjects.

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.[115] 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'.[116] In this case, the ECJ broadly interpreted the meaning of 'in the context of establishment' to avoid that fundamental rights would have been subject to a disproportionate effect due to a formal interpretation.

Thirdly, the ECJ entrusted search engines to delist online content connected with personal data of data subjects even without requiring to remove the content at stake.[117] As a result, one can argue that this interpretation has just unveiled an existing legal basis in the Data Protection Directive to enforce this right against private actors. However, by framing this decision within the new constitutional framework, the ECJ has recognised a right to be forgotten online through the interpretation of the Data Protection Directive. Such a constitutional-oriented interpretation can be considered the expression of a horizonal enforcement of the fundamental rights enshrined in the Charter. Despite this high level of protection of fundamental rights and the limitations on private actors' activities, at the same time, it is worth observing how the ECJ has delegated to search engines the task of balancing fundamental rights when assessing users' requests to delist, thus, promoting the consolidation of private ordering.[118]

These landmark decisions show the role of judicial activism in underlining the role of constitutional law in the digital environment. Nonetheless, as underlined in the case of content, judicial activism has not been enough to solve the issue raised in the field of data. The aforementioned cases just touched the constitutional challenges raised by the processing of personal data through automated decision-making technologies. Therefore, although the ECJ has contributed to the consolidation of the constitutional dimension of privacy and data protection in the Union, the next section show how the GDPR, as expression of the path of European digital

[114] Ibid, 34.
[115] Ibid, 58.
[116] Ibid, 60.
[117] Ibid, 97.
[118] Jean-Marie Chenou and Roxana Radu, 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2017) 58 Business & Society 74.

constitutionalism, has led to the codification of these judicial steps and provide a new harmonised framework of European data protection law.

4. The Third Season: Digital Constitutionalism

The changing landscape of the digital environment and the rise of new private actors online has led the ECJ to take the initiative, thus, overcoming the inertia of political power before the challenges to the protection of fundamental rights online. The ECJ's judicial activism has paved the way towards the shift from the first approach looking at digital liberalism to a new phase of digital constitutionalism characterised by the injection of democratic values in the digital environment.

This change of paradigm does not only concern the power exercise by public actors in the information society. As underlined in Chapter I, public actors are no longer the primary source of interferences with individuals' fundamental rights and freedoms. Threats for constitutional values also come from transnational private actors, precisely online platforms like social media and search engines whose freedoms are increasingly turning into forms of unaccountable power. While constitutional safeguards bind the public sector, these do not generally extend to private actors in the lack of regulation. This situation has led the Union to change its digital liberal approach to face new private forms of authority based on the exploitation of new automated technologies for processing content and data on a global scale.[119] This reaction is not only linked to the challenges for the protection of fundamental rights, such as freedom of expression and data protection by transnational corporations.[120] Even more importantly, this scenario raises concerns for the democratic system and, primarily, the principle of rule of law.[121]

Within the European framework, this new constitutional phase is based on two primary characteristics. Firstly, the Union has started to codify the ECJ's efforts. Secondly, the Union introduced new limits to online platforms' powers by adopting legal instruments to increase the degree of transparency and accountability in content moderation and data processing. Both of these characteristics can be found in the Digital Single Market strategy.[122] According to the Commission, online platforms should 'protect core values' and increase 'transparency and fairness for maintaining user trust and safeguarding innovation'.[123] The role of online platforms in the digital environment implies 'wider responsibility'.[124] 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

[119] Luciano Floridi, *The Fourth Revolution How the Infosphere Is Reshaping Human Reality* (Oxford University Press 2014).
[120] Gunther Teubner, 'The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors' (2006) 69(3) Modern Law Review 327.
[121] Paul Nemitz, 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) 376 Philosophical Transaction of the Royal Society A.
[122] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe COM(2015) 192 final.
[123] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe COM(2016) 288 final.
[124] Ibid.

content and processing data.[125] 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'.[126] Even the European Parliament proposed to better clarify the boundaries of online intermediaries' liability and guidance to define their responsibilities.[127]

This political approach resulted in a new wave of soft-law and hard-law instruments whose objective is, *inter alia*, to regulate online platforms' activities in the field of content and data by introducing new obligations and users' rights. Like other fields such as net neutrality or the right to Internet access,[128] the introduction of new users' rights constitutes the expressions of key values of the contemporary society.[129] In this sense, it would be possible to underline how Europe is living a new constitutional moment. Precisely, the Directive on copyright in the DSM ('Copyright Directive'),[130] the amendments to the audiovisual media services Directive ('AVMS Directive'),[131] the proposal for regulation to tackle online terrorist content ('Regulation on Terrorist Content'),[132] and the adoption of the GDPR are just some of the examples demonstrating how the European approach aims to protect fundamental rights and limit the power of online platforms in the algorithmic society. The next subsections show how the Union has started to introduce obligations and safeguards to limit platforms' power in the field of content and data.

4.1 Safeguards in Content Moderation

Within the framework of the Digital Single Market strategy, the Commission has oriented its efforts towards fostering transparency and accountability in the field of content. To reach this objective, the Commission adopted a fragmented approach to content moderation to reduce the discretion of online platforms to organise and remove content while mitigating the threats to users' fundamental rights.

For the first time after almost twenty years, the adoption of the Copyright Directive has changed the system of liability established by the e-Commerce Directive but applying to online

[125] Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries CM/Rec(2018)2.
[126] Ibid, 7.
[127] European Parliament resolution of 15 June 2017 on online platforms and the digital single market, 2016/2276(INI).
[128] Luca Belli (ed.), *Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking, and Traffic Management* (FGV Direito Rio 2016).
[129] Christoph B. Graber, 'Bottom-Up Constitutionalism: The Case of Net Neutrality' (2017) 7 Transnational Legal Theory 524.
[130] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130/92
[131] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities OJ L 303/69.
[132] 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)).

content-sharing service providers and limited to the field of copyright.[133] This step can considered a watershed in the European policy, acknowledging that the activities of some online platforms (e.g. social media) cannot be considered passive any longer. The digital environment has gained in complexity. The services offered by online intermediaries allow access to a large amount of copyright-protected content uploaded by their users. Likewise, online platforms have become the primary source of access to content online, generating challenges when copyright-protected content is uploaded without prior authorisation from rightholders.[134]

Since rightholders bear financial losses due to the quantity of copyright-protected works uploaded on online platforms without prior authorisation, the Copyright Directive establishes, *inter alia*, a licensing system between online platforms and rightsholders.[135] Precisely, the Copyright Directive 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 authorisation is granted, online content-sharing service providers can be held liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works unless they comply with the new conditions defining the exemption of liability.[136]

The heritage of the ECJ rulings in terms of proportionality safeguards is evident as influenced by the decisions in *Scarlet* and *Netlog*. The Copyright Directive does not introduce a general system applying to all information society services like the e-Commerce Directive, but it tries to strike a fair balance between the interests of rightsholders, the protection of users' rights and the freedom to conduct business, especially concerning small platforms. 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'.[137] 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.[138] Furthermore, the Copyright Directive extends the ban on general

[133] Martin Husovec, 'How Europe Wants to Redefine Global Online Copyright Enforcement' in Tatiana E. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* 513 (Wolter Kluwer 2019); Thomas Spoerri, 'On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market' (2019) 10(2) Journal of Intellectual Property, Information Technology and E-Commerce Law 173.Giancarlo Frosio and Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' in Giancarlo Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability* 544 (Oxford University Press 2020).

[134] Giancarlo Frosio, 'The Death of "No Monitoring Obligations": A Story of Untameable Monsters' (2017) 8(3) Journal of Intellectual Property, Information Technology 212.

[135] Copyright Directive (n 130), Art 2(6).

[136] Ibid, Art 17. When the online content-sharing service provider has not obtained an authorisation from the rightsholder, it is not liable if: '(a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from, their websites the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b)'.

[137] Ibid, Art 17(5).

[138] Ibid, Art 17(6).

monitoring not only to Member States but also the cooperation between rightsholders and online platforms.[139]

This new system of liability is not the sole novelty. The Union has not only codified the findings of the ECJ but, even more importantly, 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. Firstly, the Directive requires online content-sharing service providers to provide rightholders at their request with adequate information on the functioning of their practices with regard to the cooperation referred to and where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.[140] Moreover, these providers should put in place an effective and expeditious complaint and redress mechanism that is available to 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 them.[141] Where rightholders request to have access to their specific works or other subject matter disabled or those works or other subject matter removed, they shall duly justify the reasons for their requests.[142] In general, complaints have to be processed without undue delay, and decisions to disable access to or remove uploaded content is subject to human review. Member States are also required to ensure that out-of-court redress mechanisms are available for the settlement of disputes.[143] Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies.

The Copyright Directive shows how the Union has, on the one hand, codified the lessons of the ECJ in terms of proportionality and, on the other hand, has limited the exemption of liability of some online platforms concerning copyright-protected content. Likewise, the amendment to the audiovisual media services directive aims to increase the responsibilities of video-sharing platforms.[144] Unlike the Copyright Directive, the AVMS Directive specifies that video-sharing platforms' liability is subject to the provisions of the e-Commerce Directive.[145] As a result, the AVMS Directive has not introduced a specific liability of online platforms hosting audiovisual media services. Besides, Member states cannot oblige providers to monitor content or impose other active engagements.

Nonetheless, the AVMS Directive introduces further safeguards. Member states should ensure that video-sharing platform providers introduce 'appropriate measures' to achieve the objectives to protect minors from harmful content and the general public from audiovisual content which incite to hate against a group referred to Article 21 of the Charter or constitute specific criminal offences under EU law.[146] Such appropriate measures should also regard audiovisual commercial

---

[139] Ibid, Art 17(8).
[140] Ibid.
[141] Ibid, Art 17(9).
[142] Ibid.
[143] Ibid.
[144] AVMS Directive (n 131), Art 1(1)(b).
[145] Ibid, Art. 28a(1).
[146] Ibid, Article 28a(1)(c), namely public provocation to commit a terrorist offence within the meaning of Art 5 of Directive 2017/541/EU, offences concerning child pornography within the meaning of Art 5(4) of Directive 2011/93/EU and offences concerning racism and xenophobia within the meaning of Art 1 of Framework Decision 2008/913/JHA.

communications that are not marketed, sold or arranged by those video-sharing platform providers. In this case, the AVMS Directive clarifies that it is necessary to take into consideration 'the limited control exercised by those video-sharing platforms over those audiovisual commercial communications'.[147] Another provision regards the duty of video-sharing platform providers to clearly inform users of the programmes and user-generated videos that contain audiovisual commercial communications, where the user who has uploaded the user-generated video in question declares that such video includes commercial communications or the provider has knowledge of that fact.

As already mentioned, the measure introduced by the Member states shall comply with the liability regime established by the e-Commerce Directive. The meaning of 'appropriate measure' is specified by the AVMS Directive.[148] Precisely, the nature of the content, the possible harm which may cause, the characteristics of the category of person to be protected, the rights and the legitimate interests of subjects involved, including also those of video-sharing platforms and users, and, the public interest should be considered. Such appropriate measures should also be practicable and proportionate, taking into consideration the size of the video-sharing platform service and the nature of the service provided. The AVMS Directive provides a list of appropriate measures such as the establishment and of mechanisms for users of video-sharing platforms to report or flag to the video-sharing platform provider or age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors. The role of Member states is to establish mechanisms to assess the degree of appropriateness of these measures through their national regulatory authorities, together with mechanisms to ensure the possibility to complain and redress related to the application of appropriate measures.

In this case, the AVMS Directive has not changed the liability of video-sharing providers. Nevertheless, the aforementioned considerations show how online platforms are not more considered as passive providers but as market players whose activities should be subject to regulation. Similar observations apply to the proposal for a Regulation on Terrorist Content which aims to establish a clear and harmonised legal framework to prevent the misuse of hosting services for the dissemination of this type of content.[149] Firstly, the proposal defines terrorist content.[150] 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 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.[151]

---

[147] Ibid, Art 28a(2). The same provision extends the obligations established by Art 9 regarding audiovisual commercial communications that are marketed, sold or arranged by those video-sharing platform providers. In this case, the difference consists in the role of the video-sharing platforms that, in this case, act as a content provider exercising a control over the product and services offered.

[148] Ibid, Art 28a(3).

[149] 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> accessed 10 October 2019; 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>.

[150] Regulation on Terrorist Content (n 132), Art 2(1)(5).

[151] Ibid, Art 3.

Despite the relevance of these obligations, the implementation of these measures, described as 'duties of care',[152] 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 harbour 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.[153]

Even in this case, the Union has tried to inject procedural safeguards. 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'.[154] Hosting service providers are required, for example, to set out clearly in their terms and conditions their policy to prevent the dissemination of terrorist content.[155] Furthermore, where these providers have been subject to removal orders in that year, they shall make publicly available annual transparency reports on action taken against the dissemination of terrorist content.[156]

Transparency obligations are not the only safeguards. 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 safeguard' ensuring that content moderation is accurate and well-founded (e.g. human oversight).[157] Furthermore, it recognises the right to an effective remedy requiring online platforms to put in place procedures allowing content providers to access remedy against decisions on content which has been removed or access to which has been disabled following a removal order. As in the case of transparency obligations, this process aims to regulate content moderation.[158] Firstly, online platforms are obliged to promptly examine every complaint they receive and, secondly, reinstate the content without undue delay where the removal or disabling of access was unjustified.[159] This process is not entirely discretionary. Within two weeks from the receipt of the complaint, online platforms should not only inform the notice provider but also provide an explanation when they decide not to reinstate the content. Furthermore, in case of block or removal of terrorist content, online platforms are required to provide content providers 'comprehensive and concise information' on the removal or blocking, the possibilities to oppose this decision and a copy of the removal order issued by the competent authority.[160]

These 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

[152] Ibid,
[153] Ibid, Art 4(3).
[154] Ibid, Art 6.
[155] Ibid, Art 8(1).
[156] Ibid, Art 8(2).
[157] Ibid, Art 9(2).
[158] Ibid, Arts 9(a)-10.
[159] Ibid, Art 10(2).
[160] Ibid, Art 11.

limiting the discretion of online platforms in the field of content moderation. This observation should not lead to examine the European approach to online platforms just from a hard law perspective. These measures deserve to be framed within the attempts of the Commission to nudge online platforms to introduce transparency and accountability mechanisms.[161] The Recommendation on measures to effectively tackle illegal content online propose a general framework of safeguards in content moderation.[162] 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.[163] In the case of the removal of or blocking of access to the signalled online content, platforms should, without undue delay, inform users about the decision, stating their reasoning as well as the possibility to contest the decision.[164] 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 Digital Single Market Strategy. 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.

Although the European legal framework has made some important step forward in the field of content, however, the legal fragmentation of guarantees and remedies at supranational 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. Instead, the Union does not seem to adopt a common strategy in this field but regulate content by silos while using legal instruments which aims to reach different purposes like minimum harmonisation. It is not by chance whether there is an increasing debate about potential strategies to implement the new system of licenses introduced by the Copyright Directive.[165]

Furthermore, despite the step forward made in the last years at European level, this supranational approach has not pre-empted Member States in following their path in the field of content, precisely when looking at the law introduced by Germany in the field of hate speech,[166] and France concerning disinformation.[167] In other words, 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

[161] Code of conduct on countering illegal hate speech online (2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300> accessed 21 October 2019; Code of practice on disinformation (2018) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 25 October 2019; 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.

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

[163] Ibid, 16.

[164] Ibid, 9.

[165] João P. Quintais and others, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' (2019) 10(3) Journal of Intellectual Property, Information Technology and E-Commerce Law 277.

[166] Netzdurchsetzunggesetz, Law of 30 June 2017 ('NetzDG').

[167] 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.

constitutionalism in protecting individuals fundamental rights and limiting the powers of online platforms. This is why, as we will see in Chapter VII, the Union is working on a new legal framework in the field of content, namely the Digital Services Act.

4.2 Safeguards in the Algorithmic Processing of Personal Data

The protection of personal data has reached a new step of consolidation 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, as also resulting from the caselaw of the ECJ, 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 European data protection law.[168]

The specific focus on fundamental rights does not automatically entail neglecting other constitutional rights and freedoms at stake or even the interests of the Union in ensuring the smooth development of the internal market through promoting innovation within the context of the data industry.[169] However, it represents a change of paradigm in the approach of the Union, now focused on the fundamental rights as a beacon of data protection. 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 the system of data protection law.[170] Even when the data controller is not established in the Union,[171] 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.[172] 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 guided by the principles of the GDPR as horizontal translation of the fundamental rights of privacy and data protection. The role of the ECJ's case law is evident since the GDPR overcome formal approaches (e.g. establishment) but adopt a risk-based approach to preclude potential escape from the responsibility to protect data subjects' rights and freedoms.

Within this framework, the GDPR adopts a dynamic definition of the data controller's responsibility that considers the nature, the scope of application, the context and the purposes of the processing, as well as the risks to the individuals' rights and freedoms. On this basis, the data controller is required to implement appropriate technical and organisational measures to guarantee, and be able to demonstrate, that the processing is conducted in accordance with the GDPR.[173] The principle of accountability can be considered a paradigmatic example of how the Union has tried to inject proportionality in the field of data.

---

[168] GDPR (n 55), Recitals 1-2.
[169] Ibid, Recital 4.
[170] Ibid, Art 5.
[171] Ibid, Art 3(2).
[172] Raphael Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279; Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9(3) European Journal of Risk Regulation 502; Milda Maceinate, 'The "Riskification" of European Data Protection Law through a two-fold Shift' European Journal of Risk Regulation (2017) 8(3) European Journal of Risk Regulation 506.
[173] Ibid, Art 24.

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.[174] 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. An 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'.[175] 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 marginalised vis-à-vis the data controller. The case of the right to erasure can be considered a paradigmatic example of the codification process in the aftermath of the ECJ's case law, precisely Google Spain.[176] The right not to be subject to automated decision and the right to data portability are only two examples of the new rights upon which users can rely.[177] In other words, the provisions of new data subject's rights demonstrate how the Union intends to ensure that individuals are not marginalised 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,[178] 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'. As we will examine in Chapter VI, 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.[179] The provision of the 'human intervention' as a minimum standard in automated processing would foster the role of data subjects in the algorithmic society. In other words, this right aims to increase the degree of transparency and accountability for individuals which can rely on their right to receive information about automated decisions involving them.

However, 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

[174] Ibid, Art 25.
[175] Ibid, Art 35(3)(a).
[176] Jef Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press 2020) Silvia Martinelli, *Diritto all'oblio e motori di ricerca* (Giuffre 2017); Giulio E. Vigevani, 'Identita, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano' (2014) (4) Danno e responsabilità 741.
[177] Ibid, Arts 20, 22.
[178] Ibid, Art 22(2).
[179] Ibid, Art 22(3).

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.[180] 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 European 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 European data protection law.[181] 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. As underlined in Chapter III, the risk-based approach introduced by the 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 be considered a panacea, it constitutes an important step forward in the field of data. Like in the case of content, the Union approach has focused on increasing the responsibility of the private sector while limiting the discretion in the use of algorithmic technologies by unaccountable powers.

5. Freedoms and Powers in the Digital Environment

The advent of the Internet at the end of the last century has left its stamp on the evolution of European digital constitutionalism. The first phase of technological optimism coming from the western side of the Atlantic has spread on the other side of the ocean where the Union looked at the digital environment as an enabler of economic growth for the internal market. The evolution of the digital environment has revealed how the transplant of the US neoliberal approach to digital technologies had not taken into account the different hummus of European constitutional values, precisely when we look at the protection of fundamental rights and democratic values. This is why the first phase of digital liberalism was destined to fall before the rise of new private actors interfering with users' fundamental rights and challenging democratic values on a global scale.

It is difficult to imagine what would have been the approach of the Union if it had not followed the US path towards digital liberalism at the end of the last century. Nonetheless, the shift of paradigm is a paradigmatic example of the talent of European constitutionalism to protect fundamental rights and democratic values from the rise of unaccountable powers. From a first phase characterised by digital liberalism where freedoms were incentivised as the engine of the

[180] Margot Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529.
[181] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.

internal market, the Union's approach moved to a constitutional based approach where innovation is not the only interest to pursue. In the meantime, the ECJ has played a crucial role in this transition by building that constitutional bridge allowing constitutional values to move from the economic freedoms to fundamental rights. The Commission then codified and consolidated this shift as shown by the approach taken with the Digital Single Market Strategy.

The rise of European digital constitutionalism can be considered a reaction against the rise of private powers online. The liberal approach adopted by democratic States recognising broad areas of freedom both in the field of content and data has led to the development of business models contributing to fostering fundamental rights and freedoms online. At the same time, the price to pay for so much freedom online led to the rise and consolidation of new private powers moderating speech and processing data on a global scale based on their business interests. In other words, the liberal approach concerning the digital environment has promoted the rise of private interests competing with public powers. As we examine in Chapter III, technological evolutions, combined with a liberal constitutional approach, has led online platforms to autonomously set their rules and procedures 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). The path of European digital constitutionalism is still at the beginning. As the next chapter shows, the power exercised by online platforms, as transnational private actors, raised fundamental challenges which still need to be addressed.

Chapter III

The Law of the Platforms

Summary: 1. From Public to Private as from Atoms to Bits. – 2. A Governance Shift in the Digital Environment. 2.1 The First Constitutional Asymmetry: Democracy and Authoritarianism. 2.2 The Second Constitutional Asymmetry: Democracy and Online Platforms. – 3. Delegated Exercise of Quasi-public Powers Online. 3.1 Delegating Powers in the Content Field. 3.2 Delegating Powers in the Data Field. – 4. Autonomous Exercise of Quasi-public Powers Online. 4.1 A New Status *Subjectionis* or Social Contract. 4.2 The Exercise of Autonomous Powers. – 5. Converging Powers in the Algorithmic Society.

1. From Public to Private as from Atoms to Bits

In the 1990s, Negroponte defined the increasing level of digitisation as the movement from atoms to bits.[1] In general, a bit is only the sum of 0 and 1 but, as in the case of atoms, the interrelations between bits can build increasingly complex structures,[2] leading to the shift from materiality to immateriality.[3] The move from the industrial to the information society is primarily due to the move from rivalrousness to non-rivalrousness of traditional products and services.[4] Put another way, the bits exchanged through the internet have driven the shift from analogue to digital technologies by creating revolutionary models to market traditional products or services and leading to wonder about the application of traditional rules to the digital environment.[5] The result is that the economy is no longer based on the creation of value through production but through information flowing on a transnational architecture governed at the intersection between public authority and private ordering.

At the end of the last century, the overwhelming majority of democratic states has adopted a liberal approach to this paradigmatic shift.[6] The rapid expansion of new digital technologies combined with the liberal choice not to address these phenomena are two of the main reasons triggering the rise of transnational private actor exercising quasi-constitutional functions. Instead of a democratic decentralised society pictured by the technology optimists at the end of the last century, the digital environment is subject to the governance by an oligopoly of private entities controlling the exchange of information and providing services which are increasingly critical for

[1] Nicholas Negroponte, *Being Digital* (Alfred A Knopf 1995).
[2] Bill Gates, *The Road Ahead* (Viking Press 1995).
[3] John P Barlow, 'The Economy of Ideas: Selling Wine Without Bottles on the Global Net' in Peter Ludlow (ed.), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press 1999).
[4] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006); Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2013).
[5] Frank H. Easterbrook, 'Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Forum 207.
[6] Rosa Hartmut, *Social Acceleration: A New Theory of Modernity* (Columbia University Press 2013); John G Palfrey, 'Four Phases of Internet Regulation' (2010) 77(3) Social Research 981.

society as large as public utilities.[7] As such, the platform-based regulation of the internet has prevailed over the community-based model.[8]

Online platforms play a crucial role in ensuring the enforcement of public policies online. The activity of content moderation and the enforcement of the right to be forgotten online are only two examples illustrating how public actors have delegated regulatory tasks to private actors in the field of content and data.[9] Online platforms enjoy a broad margin of discretion in deciding how to implement these functions. For instance, the decision to remove and consequently delete a video from YouTube is a clear interference with the user's right to freedom of expression but could also preserve other fundamental rights such as their right to privacy. However, this 'delegation' of responsibilities is not the only concern at stake. By virtue of the governance of their digital spaces, online platforms also perform autonomous quasi-public functions without the need to rely on the oversight of a public authority, such as for the definition and enforcement of their Terms of Services ('ToS'). In both cases, online platforms freely rule the relationship with their communities while enforcing and balancing users' fundamental rights by using automated decision-making processes outside any constitutional safeguards.[10]

This situation could not be seen problematic from a constitutional standpoint. Rather, it could be considered the expression of online platforms' freedom. Platforms as private actors are not required to care about fundamental rights. This expression of freedom would not raise a constitutional concern as long as there are public safeguards to limit the power which private actors exercise on public discourse or privacy. Nonetheless, platforms are free to define and interpret users' fundamental rights according to their legal, economic and ethical framework due to the fact that there are no laws or regulations currently in place to prevent them from doing so or provide criteria for performing quasi-public functions. When economic freedoms turn into forms of private powers, the lack of regulation translating constitutional principle into binding norms could lead to troubling challenges for democratic values like transparency and the rule of law. The setting, enforcement and balancing of fundamental rights in the algorithmic society is increasingly privatised and compete with constitutional standards of protection.

Within this framework, this chapter highlights the reasons for the turning of platforms' freedoms to more extensive forms of private power. This chapter analyses the two interrelated forms through which platforms exercise powers in the digital environment: delegated and autonomous powers. The first part of the chapter analyses the reasons for a governance shift from

---

[7] Dan Schiller, 'Reconstructing Public Utility Networks: A Program for Action' (2020) 14 International Journal of Communication 4989; K. Sabeel Rahman, 'The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept' (2018) 39 Cardozo L. Rev. 1621; Alex Moazed and Nicholas L Johnson, *Modern Monopolies: What It Takes to Dominate the 21st Century Economy* (St Martin's Press 2016); Robin Mansell and Michele Javary, 'Emerging Internet Oligopolies: A Political Economy Analysis' in Arthur S Miller, Warren J Samuels (eds), *An Institutionalist Approach to Public Utilities Regulation* (Michigan State University Press 2002).

[8] Orly Lobel, 'The Law of the Platforms' (2016) 101 Minnesota Law Review 87.

[9] Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2017) 82(1) Brooklyn Law Review 105.

[10] Regarding technological enforcement, see Lawrence Lessig, *Code: And Other Laws of Cyberspace. Version 2.0* (Basic Books 2006); Tarleton Gillespie, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J Boczkowski and Kirsten A Foot, *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014); Helen Nissenbaum, 'From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?' (2011) 26 Berkley Technology Law Journal 1367.

public to private actors in the digital environment. The second part examines delegated powers in the field of content and data while the third part focuses on the exercise of autonomous powers competing with public authority.

2. A Governance Shift in the Digital Environment

In the last twenty years, global trends have underlined different patterns of convergence,[11] usually named 'globalisation' where the state-centric model has started to lose its power.[12] The decay of national sovereignty and territorial borders is represented by 'a world in which jurisdictional borders collapse, and in which goods, services, people and information "flow across seamless national borders"'.[13] It is no by chance whether scholars have started to refer to the rise of 'global law' to define a meta-legal system where different organisations and entities produce and shape norms with extraterritorial implications.[14]

Constitutions traditionally embody the values and principles to which a specific community decides to adhere and respect. They represent an expression of the social contract between public power and citizens. Constitutions have seen the light in different context through different forms of constituent powers.[15] Nevertheless, it is possible to underline the intimate relationship between constitutions and certain area of space (i.e. territory) over which the sovereign power is exercised and limited. The relationship between (constitutional) law and space is intricate. The law stands on a certain territorial space and relies on political processes legitimising its creation. Formally, outside the domestic legal framework, there are not any other legitimised binding forces over a certain territory unless authorised by the legal framework itself. Substantially, the law is only one of the subsystems influencing space. By abandoning a unitary view of the law as the result of the political production, it cannot be neglected how other systems tend to develop their norms.

This twofold-poietic relationship is based on the idea that the law is not a monolith but one of the systems interacting with other functional social subsystems. Although social subsystems tend to be normatively closed since they autonomously develop their rules, however, these systems are cognitively open.[16] Therefore, law, economics, technology, science and politics develop their own rule in their environment through their institutions (i.e. normatively closed) but, at the same time, they can observe other systems and be indirectly affected by them (i.e. cognitively open). This form of *autopoiesis* leads to look at the law not just as the only legitimated political structure in a certain territory but as one of the fragments composing the constitutional puzzle on a global scale.

An interesting example of this phenomenon can be found in the digital environment or the so-called 'cyberspace'. At the end of the last century, Johnson and Post wrote that '[c]yberspace

[11] Neil Walker, *Intimations of Global Law* (Cambridge University Press 2015); Maria Rosaria Ferrarese, *Prima Lezione di diritto globale* (Laterza 2012); Francesco Galgano, *La globalizzazione nello specchio del diritto* (Il Mulino 2005).
[12] Eric C Ip, 'Globalization and the Future of the Law of the Sovereign State' (2010) 8(3) International Journal of Constitutional Law 636.
[13] Ran Hirschl and Ayelet Shachar, 'Spatial Statism' (2019) 17(2) International Journal of Constitutional Law 387, 1-2.
[14] Giuliana Ziccardi-Capaldo, *The Pillars of Global Law* (Ashgate 2008).
[15] Mattias Kumm, 'Constituent Power, Cosmopolitan Constitutionalism, and Post-Positivist Law' (2016) 14(3) International Journal of Constitutional Law 2016.
[16] Gunther Teubner, *Law as an Autopoietic System* (Blackwell 1993).

radically undermines the relationship between legally significant (online) phenomena and physical location'.[17] This is why the cyberspace was considered a self-regulatory environment where bottom-up regulation replaces top-down rules by public authorities lacking any power, effects, legitimacy and notice. Besides, unlike top-down norms affected by a high degree of rigidity and uniformity, bottom-up rules ensures more flexibility. Therefore, self-regulation would provide a better regulatory framework rather than centralised rulemaking.[18]

These positions, representing the gap between law and space, is one of the reasons for the shared critics of those scholars firmly denying the idea of cyberspace as a new 'world' outside the influence of sovereign States.[19] Territorial boundaries are known for their ability to define limited areas where States can exercise their sovereignty. In the case of constitutions, these legal sources provide the rules and the principles which bind citizens to a certain sovereign space. Inside a certain territory, people are expected to comply with the applicable law in that area. The digital environment is not outside this constitutional framework. Rather than a 'lawless place', States have shown their ability to impose their sovereignty, especially by regulating network architecture.[20] In the case of China, the adoption of the 'Great Firewall' is one of the most evident examples of how states can express their sovereign powers over the internet by regulating the network's architectural dimension.[21] Precisely, it is the regulation of the online architecture the way to express powers in the digital environment.[22] According to Reidenberg, the architecture of the cyberspace prescribes its rules constituting the basis of the digital regulation,[23] while also providing instruments of regulation.[24]

Nonetheless, these arguments neglected that, although public authorities can exercise their sovereign powers over the digital environment within their territories, at the same time, other subsystems contribute to producing their norms in turn. It is not by chance whether scholars identified a 'trend toward self-regulation'.[25] More specifically, this autopoietic trend in the cyberspace would derive from the code's architecture playing the role of a set of rules constituting

---

[17] David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367.

[18] I. Trotter Hardy, 'The Proper Legal Regime for "Cyberspace"' (1994) 55 University of Pittsburgh Law Review 993.

[19] Joseph H. Sommer, 'Against Cyberlaw' (2000) 15 Berkeley Technology Law Journal 1145; Jack L. Goldsmith, 'Against Cyberanarchy' (1999) 40 University of Chicago Law Occasional Paper 1; Andrew Shapiro, 'The Disappearance of Cyberspace and the Rise of Code' (1998) 8 Seton Hall Constitutional Law Journal 703; Tim Wu, 'Cyberspace Sovereignty? The Internet and the International Systems' (1997) 10(3) Harvard Law Journal 647.

[20] Lawrence Lessig and Paul Resnick, 'Zoning Speech on the Internet: A Legal and Technical Model' (1998) 98 Michigan Law Review 395; Jack L. Goldsmith, 'The Internet and the Abiding Significance of Territorial Sovereignty' (1998) 5 Indiana Journal of Global Legal Studies 474; Joel R. Reidenberg, 'Governing Networks and Rule-Making Cyberspace' (1996) 45 Emory Law Journal 911.

[21] Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China' (2003) Harvard Law School Public Law Research Paper No. 62.

[22] Lessig (n 10); Francesca Musiani, 'Network Architecture as Internet Governance' (2013) 2(4) Internet Policy Review <https://policyreview.info/node/208/pdf> accessed 20 June 2018

[23] Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997-1998) 76 Texas Law Review 553.

[24] Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 912.

[25] Jack L. Goldsmith, 'The Internet, Conflicts of Regulation and International Harmonization', in Christoph Engel (ed), *Governance of Global Networks in the Light of Differing Local Values* 197 (Nomos 2000).

meta-legal norms of the digital environment.[26] As underlined by Sassen, 'Private digital networks are also making possible forms of power other than the distributed power made possible by public digital networks'.[27] Likewise, Perrit underlines the dispersion of governance in the cyberspace among a variety of public and private institutions.[28]

Since social subsystems can influence each other despite their process of autopoiesis, understanding the overlapping points between different subsystems becomes crucial to understand the relationship of power in the digital environment. Unlike the static vision of the 'pathetic dot',[29] organisations belonging to different social subsystems can be considered 'active dots' since they contribute to define their rules and express regulatory powers over other subsystems.[30] The relationship between entities in the cyberspace is more complicated than it appears. Firstly, it is impossible to identify one single homogeneous community: there are different micro-communities which are isolated and independently interact without knowing each other.[31] However, there are some points in the network where communities overlap. In those places, it is possible to look at the exercise of powers over the information flow. Examples of these points are Internet service providers, search engines as Google, social network platforms as Facebook or Twitter, Governments, and other private organisations. All these actors participate in shaping the environment where communities meet creating rooms of sharing values and ideas. As underlined by Greenleaf, regulating the architecture of the cyberspace is not a neutral activity but reflect the values of its governors.[32]

Notwithstanding all the actors contribute to shaping the overall picture, nodes have not the same influence on the network. Some dots in the network play the role of gatekeepers,[33] affecting the structure of the cyberspace more than others. According to Network Gatekeeper Theory's scholars, '[a]ll nodes are not created equal. Nodes vary in their accessibility, their efficacy, the other nodes they can influence and how that influence is exerted…The capacity of a node to influence or regulate depends in large part upon its resources broadly defined to include a wide range of forms of capital in the Bourdieuian sense'.[34] The node's structure plays a fundamental role in the functioning of societies. Briefly, this model does not consider the individual isolated in a specific environment, but every subject is part of a node which has the power to govern the network. Nodes have not the same dimension or the same degree of development but, as centre

[26] Lessig (n 10).
[27] Saskia Sassen, 'On the Internet and Sovereignty' (1998) 5 Indiana Journal of Global Legal Studies 545, 551.
[28] Henry H. Perritt, 'Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?' (1997) 12 Berkeley Technology Law Journal 413.
[29] Lawrence Lessig, 'The New Chicago School' (1998) 27(2) The Journal of Legal Studies 661.
[30] Andrew Murray, *The Regulation of Cyberspace* (Routledge 2007).
[31] Cass R. Sunstein, *Republic.com 2.0* (Princeton University Press 2007).
[32] Graham Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 2(2) University of New South Wales Law Journal 593.
[33] Karine Barzilai-Nahon, 'Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control' (2008) 59(9) Journal of the American Society for Information Science and Technology 1493.
[34] Scott Burris, Peter Drahos and Clifford Shearing, 'Nodal governance' (2005) 30 Australian Journal of Legal Philosophy 30.

of power, they share some common features: strategy to govern (mentalities), modalities to govern (technologies), definition of funds (resources) and structure (institutions).[35]

One of the examples where this model applies is the State. Governments define the strategy and modalities to govern, choose the resources needed to make them effective and it has a structure to execute its decisions. This model can also be applied to other entities. Some actors can exercise a stronger influence over the structure of the cyberspace than other dots. In other words, by virtue of their 'gravity', some actors in the network can attract other active dots shaping online communities and, as a result, the entire network.[36] These actors are usually called macro-nodes or gatekeepers.[37] In other words, these actors mediate in a horizontal manner between different spheres, for example, the State, the market and the community.[38] For instance, Governments are powerful actors influencing and attracting other nodes. However, the influence of Governmental nodes varies depending on the country considered. In States with a high degree of public intervention in the Internet sector like China or the Arabic States, it is clear that the weight of these nodes is more relevant than in other countries where public restrictions need to be justified and based on the law like in democratic States. Online platforms are another example of powerful nodes which can impose their rules over the digital environment by defining and enforce their standards. The differences of the nodes' weight confirm what has been analysed before: communities are dynamic concepts whose evolution is the consequence of the relations between systems.[39]

Despite the ability of this subsystem to create their own space, these organisations do not generate their rule outside any logic but are influenced by other forces including (constitutional) legal norms. The law, as a social subsystem, influences other environments. Usually, recognised powers derive from legal categories such as rules, authority or rights and freedoms. These definitions do not exist outside the legal framework but are created by the law. The notion of 'space' and 'cyberspace' is legally constituted and shaped over time in a process of legal constitutivity.[40] In other words, the peculiarity of the law as a social subsystem is to define spaces representing delegated and autonomous manifestations of powers. It is precisely when constitutionalism overcomes state boundaries and penetrated the transnational context, including the private sector, that it changes itself losing a state-centric perspective and leading to processes of 'constitutionalisation without the state'.[41] According to Teubner, this process cannot be understood just from the perspective of traditional public institutions but it can be considered as the expression of different autonomous sub-systems of the global society.[42] In the case of the digital environment, social, technical and legal processes intertwine with the result that the

[35] Less Johnston and Clifford Shearing, *Governing Security. Explorations in Policing and Justice* (Routledge 2003).
[36] Andrew Murray, 'Nodes and Gravity in Virtual Space' (2011) 5(2) Legisprudence 195.
[37] Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24(3) International Review of Law, Computers & Technology 263.
[38] Julia Black, 'Constitutionalising Self-Regulation' (1996) 59(1) The Modern Law Review 24.
[39] Murray (n 36).
[40] David Delaney 'Legal Geography I: Constitutivities, Complexities, and Contingencies' (1996) 39(1) Progress in Human Geographies 96.
[41] Gunther Teubner, 'Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?' in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism* 3, 8 (Hart 2004).
[42] Ibid.

governance of these spaces is the clash of different rationalities where the architecture constitutes the paradigm of power.

The scope of the norms produced by social subsystems is not equal across the globe but is affected by the legal environment in which these norms are created. It is no by chance whether this kind of norms tend to flourish in liberal democracies since these systems are characterised by general tolerance for pluralism and the principle of equality. On the opposite, these self-autonomous systems are weaker in authoritarian regimes where tolerance is replaced by instruments of control and surveillance.

The difference between democratic and authoritarian States is not the only asymmetry in the digital environment. New entities operating in the digital environment, precisely online platforms, enjoy new areas of power deriving not just from a mix of business opportunities and technologies,[43] but also from the openness of democracies oriented to digital liberalism which has led to delegating powers to private actors operating online. Whilst authoritarian countries have maintained their role in regulating online activities, on the opposite, as far as democratic States are concerned, their approach devoted to digital liberalism has led to the enhance the role of other social subsystems able to develop their system of governance. A new phase of liberalism based on a fundamental transformation of towards privatisations and deregulations has triggered the development of new space of power operating in the digital environment.[44] In other words, legal tolerance characterising democratic States has played a crucial role in defining a form of platform geography, a space influenced by legal frameworks where these actors self-generate their own rules on a global scale. This process could be described not only just by 'the annihilation of law by space',[45] but also 'the annihilation of law by law'. From a socio-legal perspective, this phenomenon can be considered as 'the constitutionalisation of a multiplicity of autonomous subsystems of world society'.[46] In order to better understand how the shift of powers from public to private actors primarily concerns democratic States, the next subsections focus on two constitutional asymmetries characterising the relationship between democratic systems and, on the one hand, authoritarianism and online platforms, on the other hand.

2.1 The First Constitutional Asymmetry: Democracy and Authoritarianism

The constitutional asymmetry between democracy and authoritarianism provides an interesting perspective to understand the challenges raised by private powers for constitutional democracies. Particularly in countries where forms of surveillance and control over information are diffused, like China and the Arab states,[47] the internet has been subject to public controls leading to the monitoring of data,[48] or to Internet shutdowns.[49] States around the world have not taken the same

[43] Nicolas Suzor, *Lawless The Secret Rules That Govern our Digital Lives* (Cambridge University Press 2019).
[44] Joshua Barkan, 'Law and the Geographic Analysis of Economic Globalization' (2011) 35(5) Progress in Human Geography 589.
[45] Bruce D'Arcus, 'Extraordinary Rendition, Law and the Spatial Architecture of Rights' (2014) 13 ACME: An International E-Journal for Critical Geographies 79.
[46] Teubner (n 41), 3.
[47] Barney Warf, 'Geographies of Global Internet Censorship' (2011) 76 GeoJournal 1.
[48] Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 64(3) Emory Law Journal 677.
[49] Giovanni De Gregorio and Nicole Stremlau, 'Internet Shutdowns and the Limits of Law' (2020) 14 International Journal of Communication 4224.

road towards a free-market approach to the internet which Johnson and Post identified as the solution for the governance of the cyberspace.[50] Authoritarian and totalitarian countries has shown how public actors can regulate the digital environment, thus, confirming the paternalistic theories of those scholars who have criticised the libertarian approach,[51] and considered network architecture as the primary source of regulatory powers.[52]

Unlike democracies which considered the Internet as an instrument which can foster fundamental freedoms and rights, primarily freedom of expression, authoritative regimes have shown fewer concerns in censoring the digital environment. It is possible to observe that censoring measures have been adopted particularly by those states whose authoritative regimes are not bound by constitutional limits.[53] In such cases, internet censorship is merely a political decision to protect a general national interest prevailing over any other fundamental right or conflicting interest with the regime. Authoritarianism is characterised by the presence of a central authority whose primary goal is to protect its power by dissolving any personal freedoms and other constitutional values and principles such as the rule of law.[54] Within this framework, the lack of pluralism and democratic institutions does not promote any form of freedom whose boundaries can extend so broadly to undermine central authority. It is also worth observing that authoritarianism differs from totalitarianism. Unlike totalitarianism where the central authority exercises a total power without any form of disobedience, authoritarianism is more underhand so that it is not easy to distinguish incorrect forms from practices of democracy.[55] Authoritarian countries do not deny constitutional principles and limits but manipulate them as an instrument to pursue political purposes transforming political constitutions into façade.[56]

In the lack of any safeguard and tolerance for pluralism, censoring the digital environment is not a matter of freedom and right any longer, but is equated to other discretionary measures implemented for political purposes. Therefore, it should not surprise whether the first aim of authoritarian regimes is to suppress or control the degree of pluralism to avoid any interference with the central authority. The internet is a paradigmatic example of the pluralism which authoritarian states aim to suppress. For instance, the example of Internet shutdowns or less intrusive forms of digital censorship like the suppression of false content have shown how Governments implement these practices without providing explanations or relying on a general legal basis.[57]

---

[50] Johnson and Post (n 17).
[51] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).
[52] Lessig (n 10); Reidenberg (n 23).
[53] Justin Clark and others, 'The Shifting Landscape of Global Internet Censorship' (2017) Berkman Klein Center for Internet & Society Research Publication <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425> accessed 15 October 2018; Ronald Deibert and others, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008).
[54] Tom Ginsburg and Alberto Simpser (eds), *Constitutions in Authoritarian Regimes* (Cambridge University Press 2014).
[55] Jerzy W. Borejsza and Klaus Ziemer (eds), *Totalitarian and Authoritarian Regimes in Europe: Legacies and Lessons from the Twentieth Century* (Berghahn 2007); Juan J. Linz, *Totalitarian and Authoritarian Regimes* (Lynne Rienner 2000).
[56] Giovanni Sartori, 'Constitutionalism: A Preliminary Discussion' (1962) 56(4) The American Political Science Review, 853.
[57] Ben Wagner, 'Understanding Internet Shutdowns: A Case Study from Pakistan' (2018) 12 International Journal of Communication 3917.

In the opposite scenario, democratic States are open environments for pluralism. The expression 'liberal democracy' evokes values and principles as liberty, equality, liberalism and participation rights. On the contrary, as already underlined, authoritarianism is based on narratives based on public interests, paternalism and pragmatic decision-making. Unlike authoritarian regimes, where constitutional guarantees could be absent or neglected, in democratic States, the respect of fundamental rights and freedoms is at the basis of the entire democratic system. Without protecting equality, freedom of expression or assembly, it would not be possible to enjoy a democratic society. This shows why fundamental rights and democracy are substantially intertwined. Because of this substantive relationship, fundamental rights cannot easily be exploited to pursue particular political ends.[58]

This fundamental pluralist need underlines the asymmetry between democracy and authoritarianism. It also provides clues why the concerns about the rise of private powers online primarily concern constitutional democracies. This first constitutional asymmetry has led democracies and authoritarian regime to deal with the digital environment in two different ways. While authoritarian countries have focused on developing their digital political economy controlling the market and platforms like in the case of China,[59] democratic states need to strike a fair balance between different rights and interests at stake like the freedom to conduct business of online platforms or freedom of expression. The digital environment is a crucial vehicle to foster fundamental rights and freedoms, especially through the services offered by private actors like social media and search engines. It is one of the primary sources of entertainment and knowledge allowing people to freely enjoy their freedom of expression online. Intervening in this market would need to assess not only the drawbacks for innovation but also the potential disproportionate interference with economic freedoms and fundamental rights.

However, the liberal framework driving constitutional democracies firmly clashes with the consolidation of private powers in governing the flow of information online and developing new instruments of surveillance based on the processing of vast amounts of personal data. The spread of disinformation and the misuse of data are only two examples of the challenges raised by the role of private actors in the digital environment.[60] Within this framework, democratic States are not free to restrict freedom by imposing their authority without balancing the interests at stake while private actors perform their business without being bound by constitutional limits. Within this framework, it is worth focusing on the second constitutional asymmetry concerning the different position of public and online platforms in constitutional democracies.

2.2 The Second Constitutional Asymmetry: Democracy and Online Platforms

Unlike authoritarian regimes, democratic States cannot freely adopt general censoring measures, but they are required to ensure the protection of fundamental rights and freedom if they want to safeguard democratic values. For instance, from a European constitutional standpoint, Member

[58] Susan Marks, *The Riddle of All Constitutions: International Law, Democracy, and the Critique of Ideology* (Oxford University Press 2004).
[59] Yun Wen, *The Huawei Model: The Rise of China's Technology Giant* (University of Illinois Press 2020).
[60] Giovanni Pitruzzella and Oreste Pollicino, *Hate Speech and Disinformation: A European Constitutional Perspective* (Bocconi University Press 2020).

States are required to respect the freedom to conduct business as recognised by the Charter,[61] and the Treaties protecting fundamental freedoms, especially, the freedom to provide services.[62]

This constitutional framework constitutes a crucial barrier to disproportionate regulatory attempts in the field of online platforms. Each attempt to regulate online platforms should comply with the test established the Charter according to which 'any limitation on the exercise of the rights and freedoms […] must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[63] Therefore, in order to restrict online platforms' freedoms, it is necessary that limitations comply with the principle of legality, legitimacy and proportionality. Moreover, regulatory attempts are not only blocked by economic freedoms but also by the impact that regulation could have on freedom of expression, privacy and data protection of users. According to the Charter, 'nothing in this Charter shall be interpreted as implying any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms recognised in this Charter or at their limitation to a greater extent than is provided for herein'.[64] Therefore, when addressing the challenges raised by online platforms, the Union cannot grant absolute protection just to economic freedoms or other fundamental rights. Instead, it should be avoided that the enjoyment of one fundamental right such as freedom of expression, privacy or data protection lead to the destruction of other constitutional values. This characteristic is the result of the role of dignity in European constitutionalism which does not tolerate that the core of rights and freedoms is annihilated to pursue a certain constitutional interest.[65]

In the US, the protection of online platforms activities is even broader since the constitutional ground to perform their business is based on the right to free speech as recognised by the First Amendment. Precisely, the US Supreme Court applies a strict scrutiny test according to which any such law should be narrowly tailored to serve a compelling state interest like the case *Reno v. ACLU* has already shown at the end of the last century.[66] Despite the differences between the two models, in both cases, online platforms enjoy a 'constitutional safe area' whose boundaries can be restricted only by a disproportionate prominence over other fundamental rights. Despite the passing of years and opposing positions, this liberal approach has been reiterated more recently in *Packingham v North Carolina*.[67] In the words of Justice Kennedy: 'It is cyberspace – the "vast democratic forums of the Internet" in general, and social media in particular'.[68] Therefore, social media enjoy a safe constitutional area of protection under the First Amendment,

[61] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391, Art 16.
[62] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326/47, Arts 56-62.
[63] Charter (n 61), Art. 52.
[64] Ibid, Art 54.
[65] Christine Duprè, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Hart 2015).
[66] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). Oreste Pollicino and Marco Bassini, 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis', in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* 508 (Edward Elgar 2014).
[67] Packingham v North Carolina (2017) 582 U.S. ___.
[68] Ibid.

which in the last twenty years, has constituted a fundamental ban on any regulatory attempt to regulate speech online.[69]

Therefore, when addressing the challenges raised by the digital environment, democratic States cannot just rely on general political statements arguing the need to protect public security or other public interests. In order to restrict fundamental rights and freedoms, democratic States are required to comply with constitutional procedures and safeguards. Furthermore, the respect of other constitutional rights plays a crucial role in limiting the possibility to recognise absolute protection to some values rather others and promote the development of pluralism in democratic States. Unlike authoritarian countries which fear the increase of pluralism as a threat for the central authority, democracies are concerned when areas of powers can centralise and exclude any form of pluralism.

Regulating the Internet becomes a hard goal when constitutional democracies adopt neoliberal positions. Liberal ideals and democracy are incorporated in a social contract based on limiting public powers and trust between the Government and citizens. Neoliberal ideas reject market intervention, thus, reproposing a self-regulatory environment based on individual autonomy and freedom from public interferences. In the case of the digital environment, neoliberal approach considers the role of a liberal and democratic State is harmful. In any case, the role of public actors is critical to ensure democratic principles and avoid that neoliberal positions lead to the consolidation of para-constitutional institutions competing with public authorities.[70]

Historically, the first bills of rights were designed to restrict the power of public actors rather than interfere with the private sphere. As a result, constitutional provisions have been conceived, on the one hand, as a limit to the power of the State and, on the other hand, as a source of positive obligation for public actors to protect constitutional rights and liberties. Within this framework, the primary threats for individual rights and freedoms do not derive from the exercise of broad freedoms by private actors but from the States' exercise of power. The increasing areas of power enjoyed by transnational corporations like online platforms challenge this constitutional paradigm. The rapid expansion of new digital technologies and the choice of democratic States to adopt a liberal approach regarding the digital environment are two of the reasons which have led to the rise of areas of private power. Whilst authoritarian States have shown their ability to address this situation maintaining their power by implementing instruments of control and surveillance, the laissez-faire approach of democratic States has led to the emergence of new forms of powers underlining, *de facto*, a second constitutional asymmetry in the digital environment.

Instead of introducing regulation to avoid the expansion of new private powers, constitutional democracies have started delegating public functions to online platforms. These observations just introduce only some of the developments leading private actors to expand their regulatory influence over the internet. In order to understand this situation from a constitutional perspective, the next sections address the power of online platforms to exercise delegated and autonomous functions.

---

[69] See, for example, 521 U.S. 844 (n 66); Ashcroft v Free Speech Coalition (2002) 535 U.S. 234; Aschroft v American Civil Liberties Union (2002) 535 US 564.

[70] Neil W. Netanel, 'Cyberspace Self-Governance: A Skeptical View from the Liberal Democratic Theory' (2000) 88 California Law Review 401.

3. Delegated Exercise of Quasi-Public Powers Online

The rise of private powers in the digital environment can be firstly explained as the result of an indirect delegation of public functions to online platforms. The shift from public to private in the digital environment is not an isolated phenomenon, but it is the result of a general tendency towards the transfer of functions or public tasks from lawmakers to specialised actors both in the public and the private sector.[71] The end of the Second World War has seen the rise of the welfare state leading to a proliferation of an extensive bureaucracy to deal with increasingly different social need and citizens' requests in a post-new deal scenario.[72] The result of this complexity led to the rise of a new system of delegation which does not involve anymore the relationship between the law-maker and the Government (legislative-executive) but also to the rise of two new branches respectively made of public bodies such as agencies ('fourth branch') and private entities ('fifth branch') dealing with delegated public tasks. The delegation of public functions is not just a unitary phenomenon. It can include agreements between public and private actors based on public-private partnership schemes where private entities provide goods or services.[73] The case of smart cities or governmental services are clear examples of the shift of responsibilities from the public sector to private entities.[74] In other cases, the delegation of public functions consists of the creation of new (private or public) entities to perform public tasks like the provisions of products and services or the support to rule-making activities. In this case, the setting of new government corporation or agency is one of the most evident examples.[75]

More than fifteen years ago, this shift of power from public to private actors in the digital environment was still at the beginning. Scholars at the beginning of this century started to examine how public law can be extended to a multi-stakeholder and decentralised system like the Internet. Boyle already wondered whether the Internet would have led to a transformation challenging basic assumptions not only concerning economics but also constitutional and administrative law.[76] As reported by Kaplan in the aftermath of the ICANN's foundation, Zittrain referred to a 'constitutional convention in a sense'.[77] At that time it was clear that ICANN was in a position of governing the Internet architecture in 'a position to exercise a substantial degree of power over the supposedly ungovernable world of the Internet'.[78] The case of ICANN has been the first example of the delegation to agency or other entities of regulatory powers over the digital environment. Froomkin underlined how, in the case of ICANN, the Government was violating the Administrative Procedures Act (APA) and going beyond the non-delegation doctrine coming

[71] Jody Freeman and Martha Minow (eds), *Government by Contract Outsourcing and American Democracy* (Harvard University Press 2009).
[72] Cass R. Sunstein, 'Constitutionalism after the New Deal' (1987) 101 Harvard Law Review 421.
[73] Albert Sánchez Graells, *Public Procurement and the EU Competition Rules* (Hart 2015).
[74] Sofia Ranchordas and Catalina Goanta, 'The New City Regulators: Platform and Public Values in Smart and Sharing Cities' (2020) 36 Computer Law and Security Review 105375.
[75] Marta Simoncini, *Administrative Regulation Beyond the Non-Delegation Doctrine: A Study on EU Agencies* (Hart 2018).
[76] James Boyle, 'A Nondelegation Doctrine for the Digital Age?' (2000) 50 Duke Law Journal 5.
[77] Carl S. Kaplan, 'A Kind of Constitutional Convention for the Internet' The New York Times (23 October 1998) <http://www.nytimes/com/library/tech/98/10/cyber/cyberlaw/23law.html> accessed 14 December 2019.
[78] Boyle (n 76), 6.

from the interpretation of Article 1 of US Constitution and the separation of powers principle.[79] Likewise, Weinberg underlined how ICANN played the role of a public authority since 'a private entity wielding what amounts to public power may be subjected to constitutional restraints designed to ensure that its power is exercised consistently with democratic values'.[80]

These challenges had already unveiled some of the primary concerns that it could not be foreseen at that time when online platforms have not still shown their power. Nonetheless, the arguments about the limits of delegation have not been extended to online platforms. At the beginning of this century, scholars have defined the cooperation between public actors and online intermediaries as the 'invisible handshake',[81] based on the idea that public actors rely on private actors online to pursue their aims online outside constitutional safeguards. For instance, the use of online intermediaries for law enforcement purposes could support public tasks by mitigating enforcement costs and difficulties in the digital environment. In this case, online intermediaries would provide the infrastructural capabilities to pursue public policies online since they govern the digital spaces where information flow and are hosted online, no matter if they cross national borders. In other words, online intermediaries, as other private entities, was considered an instrument for public actors to ensure the enforcement of public policies online rather than a threat leading to the rise of new powers online. The size of the infrastructure they provide is of particular interest for public authorities which can benefit from the collection of online information to pursue their purposes outside public oversight.

When focusing on the digital environment, rather than a trend towards agencification, what happened at the end of the last century was an increasing recognition of the role of private actors, especially online intermediaries, in enforcing public policies online. At the beginning of this century, Reidenberg underlined the dependency of the public sector to online intermediaries. He defined three modalities to ensure the enforcement of legal rules online: network intermediaries, network engineering and technological instruments.[82] Regarding the first approach, Reidenberg has explained how public actors can rely on online platforms to ensure the enforcement of public policies online. States do not own the resources to pursue each wrongdoer acting in the digital environment. Examples in this field are peer-to-peer and torrent mechanisms which demonstrate the complexities required to investigate, prosecute and sanction millions of infringers every day. In such situations, online providers can function as 'gateways points' (or intermediaries) to identify and block illicit behaviours acting directly on the network structure. In this way, this approach allows governments to regain control over the internet using platforms as proxies to reaffirm their national sovereignty online. In the last years, different regulatory models have raised, thus, moving from traditional approaches like 'command and control' to other models,[83]

[79] A. Michael Froomkin, 'Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution' (2000) 50 Duke Law Journal 17.
[80] Jonathan Weinberg, 'ICANN and the Problem of Legitimacy' (2000) 50 Duke Law Journal 187, 217.
[81] Micheal D Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Virginia Journal of Law & Technology 1.
[82] Joel R Reidenberg, 'States and Internet enforcement' (2004) 1 University of Ottawa Law & Technology Journal 213.
[83] Ian Brown and Christopher Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013).

such as co-regulation, self-regulation and codes of conduct.[84] The choice for models outside the control of public actors comes from expertise increasingly found outside the public sector.[85]

The shift of power from the public to the private sector can be interpreted not only as the consequence of economic and technical forces but also as the result of the different influence of states in the field of internet governance.[86] Precisely, the choice to delegate public functions to online platforms is linked to the opportunity to rely on entities governing their online environment. Governments and public administration increasingly rely on big tech companies, for instance, to offer new public services or improve their quality through digital and automated solutions.[87] However, this cooperation leads, firstly, tech companies to hold a vast amount of data coming from the public sector, thus, including also those of individuals. Secondly, public actors are technologically dependent 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. Governments have forfeited sovereign power to private actors providing national services based on cloud computing and other digital infrastructure governed by the private sector.[88]

Even if online intermediaries can play a critical role in ensuring legal enforcement in the digital environment, delegating public powers empowers the private sector to set the rule of the game through a mix of law and technology. The private sector can set the technical rules and the degree of transparency of their technologies, thus, maintaining far public actors from exercising any form of oversight. It cannot be excluded that relying on the private sector offers an advantage based on corporativist expertise. In the digital environment. Online intermediaries are experts in this field, especially since they govern the space where information and data flow online. In other words, rather than adapting or creating a new administrative body to deal with public functions online, public actors have considered more convenient to rely on entities which they know how to do their job. Online platforms can indeed influence public policies due to the dependency of the public sector, especially for surveillance purposes, and the interests of citizens to access digital services which otherwise would not be offered by the public sector.

Nonetheless, no matter whether direct or indirect, the delegation of public functions to private actors touches upon some of the most intimate features of constitutional law: the constitutional divide between public and private actors, the separation of power, the principle of the rule of law and, even more importantly, the democratic system. Although the gap between public and private actors could look like formal at first glance, this distinction involves the core of constitutional law

---

[84] Monroe E. Price and Stefaan G. Verhulst, *Self-Regulation and the Internet* (Kluwer 2004).

[85] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439.

[86] Roxana Radu, *Negotiating Internet Governance* (Oxford University Press 2019).

[87] Smart cities are examples of this situation. See Robert Brauneis and Ellen P. Goodman, Algorithmic Transparency for the Smart City (2018) 20 Yale Journal of Law and Technology 103; Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 1 European Data Protection Law 26.

[88] Aaron Gregg and Jay Greene, 'Pentagon awards controversial $10 billion cloud computing deal to Microsoft, spurning Amazon' Washington Post (26 October 2019) <https://www.washingtonpost.com/business/2019/ 10/25/pentagon-awards-controversial-billion-cloud-computing-deal-microsoft-spurning-amazon/> accessed 25 September 2020.

and, especially, how constitutional provisions apply vertically only to public bodies, while private actors are not required to comply with these boundaries without any regulatory intervention. This constitutive difference can explain why the transfer of public functions (or powers) to the private sector is subject to constitutional limits. These boundaries aim to control to what extent lawmakers can transfer or delegate authority to other (public or private) entities and the constitutional safeguards that should apply to avoid a dangerous marginalisation of democratic values in favour of non-accountable logic. These challenges have already emerged in other sectors where financial institutions, telecom companies and other infrastructure owns the resources and the mean to impose private standards over public value. This concern was already expressed by Brandeis which define this situation as the 'curse of bigness' to underline the role of corporations and monopolies in the progressive era.[89] However, in the digital environment, unlike traditional forms of delegation between public and private actors, an indirect form of delegation is one of the reasons leading to the current scenario of powers exercised by private actors online.

Delegating online platforms to perform public tasks online is not problematic *per se*. It is the lack of procedural and substantive safeguards leaving the private sector free to consolidate their power. The lack of safeguards challenges democratic constitutionalism. Precisely the idea of government 'of the people, by the people, for the people' is put under pressure when public functions are left to the discretion of non-accountable private actors without any public safeguard. Looking at US constitutional law, the ban for the Congress to delegate power 'is a principle universally recognized as vital to the integrity and maintenance of the [democratic] government ordained by the Constitution'.[90] Moving to the European framework, the ECJ has clarified the boundaries of delegation from Union's institutions to agency and private actors by, *de facto*, creating a judicial non-delegation doctrine.[91] As observed by the Strasbourg Court, 'the State cannot absolve itself from responsibility by delegating its obligation to private bodies or individuals'.[92] Because 'the fact that a state chooses a form of delegation in which some of its powers are exercised by another body cannot be decisive for the question of State responsibility (..); [t]he responsibility of the respondent State thus continues even after such a transfer'.[93]

This view has indeed not only be questioned by the increasing reliance on other public bodies like agencies and independent administrative authorities to face the technocratic reality of the administrative State.[94] It has also been challenged by a general trust in the role of the private sector or rather the belief that digital liberalism would have been the most suitable approach for the digital environment at the end of the last century. This is why it is crucial that, when delegating public functions to private actors, public safeguards limit the unaccountable determinations of private actors operating transnationally. In other words, the aim of this safeguard would be to avoid a dangerous uncertainty resulting from the mix of, citing Boyle when referring to ICANN,

[89] Louis D. Brandeis, 'The Curse of Bigness', in Osmond K. Fraenkel (ed), *The Curse of Bigness: Miscellaneous Papers of Louis D. Brandeis* (Viking Press 1934). See also Tim Wu, *The Curse of Bigness: How Corporate Giants Came to Rule the World* (Atlantic Books 2020).
[90] Field v Clark 143 US 649 (1892), 692.
[91] Robert Schutze, '"Delegated" Legislation in the (New) European Union: A Constitutional Analysis' (2011) 74(5) Modern Law Review 661.
[92] Costello-Roberts v United Kingdom (1993) 19 EHRR 112 27-28.
[93] Wos v Poland (2007) 45 EHRR 28, 72.
[94] Gary Lawson, 'The Rise and Rise of the Administrative State' (1994) 107 Harvard Law Review 1231.

'public and private, technical harmonization and political policy choice, contractual agency relationship and delegated rulemaker, state actor and private corporation'.[95]

Digital liberalism has led to a shift of power and responsibility from governments to the private sector based on a trust which, however, in the lack of any safeguard, is misplaced for at least two reasons. Firstly, private actors are not bound by limits to respect constitutional values and principles such as fundamental rights. Therefore, the absence of any regulatory safeguards leads private actors free to choose how to shape constitutional values based on their business interests. Moreover, supporting self-regulation leaves the private sector free to impose standards which do not only influence public values but also private entities suffering the exercise of a horizontal forms of authority (or powers) coming from a mix of regulatory, economic and technological factors.

The next subsections underline the rise of platforms' power coming from delegation of public functions. In the field of content, the analysis focuses on the role that the liability regime of online intermediaries has played in encouraging platforms to moderate content and setting the standard of protection of freedom of expression in the digital environment. The second subsection focuses on the role of European data protection law in entrusting online platforms with discretion on the processing of personal data.

3.1 Delegating Powers in the Content Field

The first example of delegation can be found in the role of online platforms in moderating illegal content hosted in their digital spaces. At the end of the last century, by virtue of their 'passive' function, online intermediaries were treated as mere intermediaries of products and services without any responsibility for the content they host. Both the US and European approach to online intermediaries' liability are clear examples. The Communications Decency Act,[96] together with the Digital Millennium Copyright Act,[97] and the e-Commerce Directive,[98] have introduced a special regime of exceptions to the liability of online intermediaries, acknowledging, *in abstracto*, their non-involvement in the creation of content.[99]

When looking at the e-Commerce Directive, this allocation of public functions technically consists in imposing obligations to online intermediaries to remove online content once they become aware of its illicit nature ('notice and takedown'). As examined in Chapter II, public actors have generally considered platforms neither accountable nor responsible for transmitted or hosted contents (i.e. safe harbour), considering platforms unaware of the presence of illicit content in their digital rooms.[100] On the one hand, the liability of online intermediaries in relation to third-party content has always been limited to foster the development of information society services, thus protecting freedom of economic initiative (or free speech in the US framework). On the other

[95] Boyle (n 76), 8.
[96] Communications Decency Act (1996), Section 230(c)(1).
[97] Digital Millennium Copyright Act (1997), Section 512.
[98] 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.
[99] Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017).
[100] E-Commerce Directive (n 98), Arts 12-14; Communications Decency Act (n 96), Section 230.

hand, this special regime aims to avoid that entities which do not have effective control over third-party content are considered liable for hosting them.

Lacking any procedural obligations, this system of liability has entrusted online intermediaries with the power to autonomously decide whether to remove or block content based on the risk to be held liable. Since online platforms are privately run, these actors would try to avoid the risks to be sanctioned for non-compliance with this duty by removing or blocking especially content whose illicit nature is not fully evident. The case of disinformation can provide an interesting example. Since it not always possible to understand whether a false content is unlawful and eventually on which legal basis, this legal uncertainty encourages online platforms to monitor and remove even lawful speech to avoid any risk of liability.[101] This situation, named collateral censorship,[102] occurs when private actors are entrusted to remove unlawful content when they become aware of their presence. This obligation encourages online intermediaries to censor even those content whose illicit nature is not clear to avoid any economic sanctions. Such a system of liability indirectly entrusts online intermediaries to autonomously decide whether to maintain and remove content based on the risk to be held liable. Since online platforms are privately run, these actors would try to avoid the risks to be sanctioned for non-compliance. The Strasbourg Court has also underlined this risk, especially in its case law concerning the relationship between freedom of expression and online intermediaries' liability.[103] In other words, online intermediaries, as business actors, would likely focus on minimising this economic risk rather than adopting a fundamental-rights-based approach.

Therefore, such delegated activity implies, *inter alia,* that platforms can take decisions affecting fundamental rights and freedoms.[104] At the same time, this responsibility would also imply that Member States should implement effective and appropriate safeguards to ensure the prevention of unintended removal of lawful content and respect the fundamental rights in question.[105] However, this is not the current situation. The e-Commerce Directive does not provide any safeguards limiting platforms discretion. Obligations are indeed directed to Member States while online platforms, as hosting providers, they should just remove content once they become aware of their illicit presence online. The e-Commerce Directive refers to the protection of freedom of expression only when underlining its functional role to the free movement of

[101] Oreste Pollicino, Giovanni De Gregorio and Laura Somaini, 'The European Regulatory Conundrum to Face the Rise and Amplification of False Content Online' (2020) 19(1) Global Yearbook of International Law and Jurisdprudence 319.
[102] Felix T. Wu, 'Collateral Censorship and the Limits of Intermediary Immunity' (2013) 87 Notre Dame Law Review 293; Seth F. Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 University of Pennsylvania Law Review 11; Jack M. Balkin, 'Free Speech and Hostile Environments' (1999) 99 Columbia Law Review 2295.
[103] Delfi AS v. Estonia (2015); Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v Hungary (2016). According to para 86: '[…] Such liability may have foreseeable negative consequences on the comment environment of an Internet portal, for example by impelling it to close the commenting space altogether. For the Court, these consequences may have, directly or indirectly, a chilling effect on the freedom of expression on the Internet. This effect could be particularly detrimental to a non-commercial website such as the first applicant'
[104] Orla Lynskey, 'Regulation by Platforms: The Impact on Fundamental Rights' in Luca Belli and Nicolo Zingales (eds), *Platform Regulations How Platforms are Regulated and How They Regulate Us* (FGV Direito Rio, 2017); James Grimmelmann, 'Speech Engines' (2014) 98 Minnesota Law Review 868.
[105] E-Commerce Directive (n 98), Recital 42.

information society services,[106] and clarifying that the removal or disabling of access to online content has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level. It is not by chance if another Recital clarifies that Member States can require service providers to apply 'duties of care' to detect and prevent certain types of illegal activities. These provisions are not binding playing the role of interpretative guidelines, in this case, for Member States when implanting the e-Commerce Directive.

Even more importantly, when the e-Commerce Directive refers to the need that online intermediaries respect the right to free speech when they moderate content, it is not clear whether this interpretative statement refers to the protection ensured, at that time, by Article 10 of the Convention or that functional dimension linked with the need to ensure the freedom to movement of information society services. More in general, such acknowledgement contribute to entrusting online platforms with the power to enforce and adjudicate disputes in the field of online content based on a standard of protection which is not only unclear but also based on platforms' business interest.

Even if, in Chapter II, we have underlined how the Union has started to limit platforms' discretion in content moderation, several drawbacks need to be addressed. Firstly, expressions can be qualified as illegal only according to a decision coming from public authorities. If platforms are left to determine the lawfulness of online content, they are then exercising a function which traditionally belongs to the public authority. Once hosting providers become aware of the presence of alleged illicit content through users' notice or other ways, these actors are not required to remove content since no public authorities have still defined that content as unlawful. Therefore, it is the platform which assesses the lawfulness of the content in question to remove it promptly. Lacking any regulation of this process, online platforms are free to assess whether certain online content is unlawful and make a decision regarding its consequent removal or block. As a result, this anti-system has led platforms to acquire an increasing influence on the enforcing and balancing of users' fundamental rights. For example, the choice to remove or block defamatory content or hate speech videos interferes with the right to freedom of expression of the users. At the same time, the decision about the need to protect other conflicting rights such as the protection of minors or human dignity is left to the decision of private actors without any public guarantee.

Within this framework, as we will examine in Chapter V, the primary issue is the lack of any transparent procedure or redress mechanisms allowing users to appeal against a decision regarding the removal or blocking of the signalled content. For example, platforms are neither obliged to explain the reasoning of the removal or blocking of online content, nor to provide remedies against their decisions even if they process vast amounts of content. Lacking any regulation, users cannot rely on any legal remedy to complain against a violation of their fundamental rights. This situation raises concerns even for democratic systems. The choice to delegate online platforms to make decisions on content empowers platforms to influence public discourse. These private entities can autonomously set and decide the standard of protection of fundamental rights online, including the right to freedom of expression which is one of the cornerstones of democracy.

[106] Ibid, Recital 9.

3.2 Delegating Powers in the Data Field

The field of data has also experienced a process of delegation from public authorities to the private sector. Unlike the case of content, however, the primary concerns are not related to the lack of safeguards but the risk-based approach which the Data Protection Directive introduced already in 1995.[107] Besides, in this case, the delegation of public power comes not only from legal instruments but also from the ECJ's case law and, especially, the *Google Spain* decision concerning the enforcement of the right to be forgotten in the online dimension.[108]

The Data Protection Directive already had tried to introduce such an approach focused on the risk of processing. Likewise, the WP29 stressed the role of a risk-based approach in data protection underlining how risk management is not a new concept in data protection law.[109] Even the Council of Ministers of the Organisation for Economic Cooperation and Development (OECD) implemented a risk-based approach when revising the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, first adopted in 1980.[110] For instance, concerning the implementation of security measures.[111] According to the Data Protection Directive, security measures must 'ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected'.[112] Even more importantly, the assessment of risk was also considered one legal basis for the processing of personal data when the processing is 'necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects'.[113] In both cases, this assessment rests in the hands of data controller which 'determines the purposes and means of the processing of personal data'. Even, this definition can explain how the governance of personal data is not just determined by public authorities but is also firmly dependent on the choices of data controller. Unlike these cases, the relevance of risk also extends to Member States through data protection authorities to assess specific risks coming from the processing of personal data.[114]

The GDPR has indeed underlined the fallacies of European data protection law.[115] According to Koops, 'data protection law is a dead letter; current ideas what to do with the body are not leading anywhere except that they offer entertainment to spectators. With the current reform, the

---

[107] 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.
[108] Frank Pasquale, 'Reforming the Law of Reputation' (2015) 47 Loyola University of Chicago Law Journal 515.
[109] Working Party Article 29, Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks (2014).
[110] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).
[111] Christopher Kuner and others, 'Risk Management in Data Protection' (2015) 5(2) International Data Privacy Law 95.
[112] Data Protection Directive (n 107), Art 17.
[113] Ibid, Art 7(f).
[114] Ibid, Art 20.
[115] 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.

letter of data protection law will remain stone-dead'.[116] This announced death of data protection would be caused by 'the delusion that data protection law can give individuals control over their data (fallacy 1); the misconception that the reform simplifies, while in fact it makes compliance even more complex (fallacy 2); and the assumption that data protection law should be comprehensive, stretching data protection to the point of breaking, and making it meaningless law in the books (fallacy 3)'.[117]

Despite these challenges, the GDPR has opened the doors towards a comprehensive risk-based approach, especially based on the principle of accountability of the data controller. As underlined in Chapter II, the principle of accountability requires the controller to prove the compliance with GDPR's principles by establishing safeguards and limitations based on the specific context of the processing, especially on the risks for data subjects. The GDPR modulates the obligation of the data controller according to the specific context in which the processing takes place.[118] As observed by Macenaite, 'risk becomes a new boundary in the data protection field when deciding whether easily to allow personal data processing or to impose additional legal and procedural safeguards in order to shield the relevant data subjects from possible harm'.[119] It would be enough to focus on the norms concerning the Data Protection Impact Assessment,[120] or the appointment of the Data Protection Officer,[121] to understand how the GDPR has not introduced mere obligations to comply but a flexible risk-based approach which leads to different margins of responsibility depending on the context at stake.[122] In other words, the GDPR has led to the merge of a rights-based approach where the fundamental rights of the data subjects play the role of 'beacon for compliance', with a risk-based approach based on a case-by-case assessment of data controllers' responsibility.

However, the potential scope of the principle of accountability should not be neglected. Data controllers 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 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. Within this framework, the GDPR adopts a dynamic definition of the data controller's responsibility that considers the nature, the scope of application, the context and the purpose 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 organisational measures to guarantee, and be able to demonstrate, that the processing is conducted in accordance with the GDPR.[123] The principles of privacy by design and by default contributes to achieving this purpose

[116] Bert-Jaap Koops, 'The Trouble with European Data Protection Law', (2014) 4(4) International Data Privacy Law 250.
[117] Ibid, 251.
[118] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).
[119] Milda Maceinate, 'The "Riskification" of European Data Protection Law through a two-fold Shift' European Journal of Risk Regulation (2017) 8(3) European Journal of Risk Regulation 506.
[120] GDPR (n 115), Art 35.
[121] Ibid, Art 37.
[122] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279; Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9(3) European Journal of Risk Regulation 502.
[123] GDPR (n 115), Art 24

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.[124] 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."[125] 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.

Besides, the adoption of the risk-based approach can affect small or medium controllers which can be required to adopt higher safeguards, especially when data processing operations could lead to high risks for the data subjects.[126] Even if this approach could favour multinational corporations in developing more complex processing, it introduces a mechanism which does not focus only on rigid obligations but on the concrete framework of the processing. This shift from theory to practice introduces certain flexibility allowing the data controller to determine the measures to be applied according to the risks connected to data processing while maintaining the duty to justify the reasons for these decisions. As we will see in Chapter VI, therefore, this reference to a case-by-case system represents nothing but the expression of a principle of proportionality aimed to balance the conflicting interests of data controllers and data subjects. Even more importantly, the adoption of a risk-based approach empowers data controllers.

Even before the adoption of the GDPR, another form of delegation of power in the field of data comes from the ECJ when recognising for the first time the right to be forgotten online in the landmark decision *Google Spain*.[127] Even without analysing the well-known facts of the case, one can observe that such a decision finds its roots in the necessity to ensure the protection of the fundamental right to privacy in the digital dimension.[128] The court has brought out a new right to be forgotten as a part of the right to privacy in the digital world.[129] In order to achieve this aim, the ECJ, as a public actor, interpreted the framework of fundamental rights together with the dispositions of the Data Protection Directive and *de facto* entrusted private actors (in this case, search engines) to delist online content without removing information on the motion of the individual concerned. The search engine is the only actor which can ensure the enforcement of the right to be forgotten online since it can manage those online spaces where the links to be forgotten are published.

However, unlike in the case of content, both the ECJ and the EDPB (and before the Article 29 Working Party) have identified some criteria according to which platforms shall assess the request

[124] Ibid, Art 25.
[125] Ibid, Art 35(3)(a).
[126] Michal S. Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349.
[127] Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014).
[128] Ibid 84.
[129] Oreste Pollicino and Marco Bassini, 'Reconciling Right to be Forgotten and Freedom of Information in the Digital Age. Past and Future of Personal Data Protection in the EU' (2014) 2 Diritto pubblico comparato ed europeo 641.

of the data subject.[130] Thus, online platforms do not enjoy an unlimited discretion in balancing data subjects' rights. Moreover, the recent European codification of the right to erasure has contributed to clarifying the criteria to apply the right to delist. Precisely, the data subject has the right to obtain from the controller, without undue delay, the erasure of personal data concerning him or her according to specific grounds,[131] and excluding such rights in other cases,[132] for example when the processing is necessary for exercising the right to freedom of expression and information.

Although the data subject can rely on a legal remedy by lodging a complaint to the public authority to have their rights protected, the autonomy of platforms continues to remain a relevant concern. When addressing users' requests for delisting, the balancing of fundamental rights is left to the assessment of the online platforms. In Chapter IV, we will understand better how the issue is similar to that of the notice and takedown mechanism since search engines enjoy a broad margin of discretion when balancing users' fundamental rights and enforcing their decisions. Search engines decide whether the exception relating to the freedom to impart information applies in a specific case. They delist results by relying only on their internal assessments based on the facts provided by the data subject and they are not obliged to provide any reason for their decision or redress mechanism. Therefore, the online enforcement of the right to be forgotten is another example of the (delegated) discretionary power that platforms exercise when balancing and enforcing fundamental rights online. As in the case of content, this freedom does not only constitute a delegated function but also the general expression of autonomous powers outside the oversight of public authorities.

4. Autonomous Exercise of Quasi-Public Powers Online

The delegation of public functions to online platforms is not the only challenging phenomenon for the traditional boundaries of constitutional law. The autonomy afforded to online platforms in the phase of digital liberalism has led these actors to acquire areas of power beyond delegation. The technological evolution together with a liberal constitutional approach has allowed online platforms not only to become proxies of public actors but also to rely on their private autonomy to set their own rules of procedures.

In the *laissez-faire* scenario, data and information have started to be collected globally by private actors through the possibilities derived from new digital technologies, firstly, by the internet and, subsequently, by the development of automated technologies. Whereas in the information society bits have allowed private actors to gather information and develop their business, today algorithms allow such actors to process it by extracting value from vast amounts of data (or 'Big Data'). Since data and information constitute the new non-rival and non-fungible

[130] European Data Protection Board, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR, 2 December 2019; Working Party 29, 'Working Party on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12', <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> accessed 25 June 2018.
[131] Ibid art 17(1).
[132] Ibid art 17(3).

resource of the algorithmic society,[133] their processing has led to an increase in the power of some private actors in the digital age where the monopoly over knowledge does not belong exclusively to public actors but also some private businesses. Put another way, today, data is more valuable than oil: the latter is consumable while data can process without limits, thus, producing an infinite value. The possibility to autonomously set the rules according to which data flows and is processed leads to an increase in the discretion of private actors.[134] From a transnational constitutional perspective, this phenomenon can be described as the rise of a civil constitution outside institutionalised politics. According to Teubner, the constitution of a global society cannot result from a unitary and institutionalised effort but emerges from the constitutionalisation of autonomous subsystems of that global society.[135]

Although online platforms are still considered service providers, the consequences of their gatekeeping role cannot be neglected. The possibility to autonomously set the rules according to which information flows and is processed on a global scale leads to an increase in the discretion of these private actors. As Pasquale observed, online platforms 'aspire to displace more government roles over time, replacing the logic of territorial sovereignty with functional sovereignty. In functional arenas from room-letting to transportation to commerce, persons will be increasingly subject to corporate, rather than democratic, control'.[136] Daskal underlined the ability of private actors in setting the rules governing the Internet.[137] Intermediaries have increasingly raised as surveillance infrastructures,[138] as well as governors of digital expressions.[139] Therefore, these functional expressions of power increasingly compete with states' authority based on the exercise of sovereign powers on a certain territory.[140] This consideration shows why some scholars have referred to this phenomenon as the rise of the law of the platforms.[141] Put another way, online platforms have developed their private geography influencing social subsystems on a global scale.

These challenges do not concern just the role of public actors in regulating online intermediaries, but, more importantly, the possibility for democratic States to avoid the consolidation of private powers whose nature is even more global than local.[142] The consolidation of new founding powers could be dangerous for democracies. Unlike authoritarian countries

---

[133] 'The World's Most Valuable Resource Is No Longer Oil but Data' The Economist (6 May 2017) <www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 28 May 2018.
[134] Yochai Benkler, 'Degrees of Freedom Dimension and Power' (2016) 145 Daedalus 18.
[135] Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press 2012).
[136] Frank Pasquale, 'From Territorial to Functional Sovereignty: The Case of Amazon. Law and Political Economy' LPE (2017) <https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/>.
[137] Jennifer ro, 'Borders and Bits' (2018) 71 Vanderbilt Law Review 179.
[138] Alan Z. Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stanford Law Review 99.
[139] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598; Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 U.C. Davis Law Review 1151
[140] Kristen E. Eichensehr, 'Digital Switzerlands' (2018) 167 University Pennsylvania Law Review 665.
[141] Luca Belli, Pedro A. Francisco and N. Zingales, 'Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Policy' in Belli and Zingales (n 104), 41.
[142] Gunther Teubner, 'The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors' (2006) 69 Modern Law Review 327.

which fear the increase of pluralism as a threat to the central authority, democracies aim to protect pluralism and freedom. The primary challenge is when such freedom leads to the consolidation of areas of powers centralising and excluding any form of pluralism. The next subsection focuses on examining the exercise of autonomous powers by online platforms. The first part examines a new status of *subjectionis* or social contract. The second describes how platforms enjoy areas of freedoms that *de facto* represent the exercise of quasi-public powers online.

4.1 A New Status of *Subjectionis* or Social Contract

In 2017, Zuckerberg stated that 'Great communities have great leaders' and 'we need to give more leaders the power to build communities'.[143] This expression could just seem unoffensive at first glance. Nevertheless, they indirectly picture the inspirational values on which online platforms' business is based. Rather than a free environment where everyone enjoys freely the relationship inside the community and share their ideas, the idea of Facebook's CEO is that communities' success does not come from participation and involvement but the power of its leader. The will of the leader, receiving its investiture from the company, shapes communities. This narrative is far from looking democratic. However, these pharaonic statements should not surprise since online platforms, as business actors, are not keen on democratic forms of participation based on transparency and accountability. They care more to ensure a sound and stable governance driven by profit maximisation.

Therefore, the starting point to understand the exercise of autonomous powers online is to focus on how platforms regulate their users in their digital spaces. The way in which platforms set the standards of their digital spaces is not casual but the result of opaque reasons usually based on the peculiarities of their business models. At first glance, a contractual agreement governs the relationship between users and online platforms. Users decide spontaneously to adhere to the rules established in ToS and community guidelines. The increasing role of online platforms as social infrastructures annihilate any contractual power of the user. The role of online platforms in the current society is crucial on a global scale.[144] The global pandemic has shown the relevance of online platforms in the society. They contribute to offering people services, for example, to find resources online (i.e. search engines), buy product and services (i.e. e-commerce marketplaces), communicate and share information and data with other people (i.e. social media). Without considering their market power, it would be enough to look at the number of the users of Facebook or Google to understand that their community is bigger than entire regions of the world,[145] so that the definition of a 'company-town' would seem reductive.[146] The inhabitants of these digital spaces consider online platforms, especially social media, as the primary channel for news or even managing intimate and professional relationship as well as advertising their business. As Pasquale

[143] Mark Zuckerberg, 'Bringing the World Closer Together', Facebook (22 June 2017) <https://www.facebook. com/notes/mark-zuckerberg/bringing-the-world-closer-together/10154944663901634/> accessed 8 February 2020.
[144] Martin Moore and Damian Tambini (eds), *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).
[145] Anupam Chander, 'Facebookistan' (2012) 90 North Carolina Law Review 1807.
[146] Tal Zarsky, 'Social Justice, Social Norms and the Governance of Social Media' (2015) 35 Pace Law Review 154.

underlined, the real product here is users' information and data.[147] The company can exercise a form of private monitoring over content and data shared, not so differently from governmental surveillance. Likewise, Kim and Telman underline how 'private data mining is just as objectionable and harmful to individual rights as is governmental data mining',[148] and 'because corporate actors are now empowered to use their technological advantages to manipulate and dictate the terms on which they interact with the public, they govern us in ways that can mimic and even supersede governance through democratic processes'.[149] As a result, the number of users leads platforms not only to profit from information and data by feeding their business model based on advertising revenues or users' profiling. Indeed, their power is not just a matter of quantity but also of quality. In other words, online platforms have acquired their areas of power not only as resulting from the amount of data and information involved but also from their gatekeeping role based on the organisation of online spaces for billions of users.[150]

Therefore, these digital spaces are not based on horizontal systems where communities decide and shape their rules but vertical contractual relationships resembling a new *pactum subjectionis* where users bargain (*rectius* renounce to) their constitutional rights to adhere to conditions determined through a top-down approach driven by business interests. Platforms are the ruler of their digital space since they can manage the activities which occur within their boundaries, so the relationship with their digital space creates a new understanding of their geography on a global scale. It is no by chance whether ToS have been analysed as the constitutional foundation of online platforms' activities.[151] As Radin explained, generally, businesses try to exploit new form contracts to overrule legislation protecting parties' rights.[152] Contract law allows private actors to exercise regulatory authority over private relationship 'without using the appearance of authoritarian forms'.[153] According to Slawson, contracts, and especially standard forms, hide an antidemocratic tendency '[s]ince so much law is made by standard form it is important that it be made democratically'.[154] Indeed, users enter into digital spaces where private companies are 'both service providers and regulatory bodies that govern their own and their users' conduct'.[155] It is no by chance that Zuboff describes the aim of ToS as a 'form of unilateral declaration that most closely resembles the social relations of a pre-modern absolutist authority'.[156] Likewise,

[147] Frank A. Pasquale, 'Privacy, Autonomy, and Internet Platforms' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the Modern Age, the Search for Solutions* (The New Press 2015).
[148] Nancy S. Kim & D. A. Telman, 'Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent' (2015) 80 Missouri Law Review 723, 730.
[149] Ibid.,
[150] Orla Lynskey, 'Regulating Platform Power' (2017) LSE Legal Studies Working Paper 1 <http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf> accessed 1 September 2018.
[151] Edoardo Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2018) International Review of Law, Computers & Technology <https://www.tandf-online.com/doi/abs/10.1080/13600869.2018.1475898> accessed 1 December 2018.
[152] Margaret J. Radin, *Boilerplate the Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013).
[153] Fredrick Kessler, 'Contract of Adhesion - Some Thoughts about Freedom of Contract' (1943) 43 Columbia Law Review 629, 640.
[154] David Slawson, 'Standard Forms of Contract and Democratic Control of Lawmaking Power' (1967) 84 Harvard Law Review 529, 530.
[155] Omri Ben-Shahar and Carl E. Schneider, *More than You Wanted to Know: The Failure of Mandated Disclosure* 27 (Princeton University Press 2016).
[156] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75.

MacKinnon describes this situation as a Hobbesian approach to governance, where users give up their fundamental rights to access and enjoy digital services.[157] In other words, moving from private to constitutional law, platforms vertically govern their communities and the horizontal relationship between users through a mix of instruments of technology and contract law.[158]

This process is mostly opaque for the average user. Since some platforms play the role of monopolist in the markets, users cannot see other ways rather than adhering with unilateral conditions. The mix of automated technologies of moderation, internal and community guidelines and technological reproduces a system of constitutional rules and principles governing communities. As Evans explains that the rules and penalties imposed by the platform mirror (and, in some cases, substitute) those adopted by public authorities.[159] In this para-constitutional framework, the vertical and horizontal relationship of users and, therefore, the exercise of their rights and freedoms are privately determined without the substantive and procedural safeguards democratic constitutional norms traditionally offer. Within this authoritarian framework, as observed by Shadmy, 'corporate services […] transforms rights in the public imaginary into privileges that the company grants and can revoke, according to its own will and interest'.[160]

Besides, the power to shape and determine fundamental rights and freedoms in the digital environment is not the only concern. By looking at the relationship with users, it is possible to obtain other clues to support that the activities of online platforms mirror an absolute regime rather than a private constitutional order. Individuals do not only enjoy rights but, as citizens, they contribute to defining the values of their communities through democratic process such as representation. This political form of participation is one of the primary differences with online platforms' communities.[161] Rights and freedoms have been powerful forces which have guided the evolution of liberal and, then, democratic constitutionalism. From US constitution to the Declaration of the Rights of Man and Citizens at the end of the eighteenth century, constitutions were conceived as ways to limit power, organise the relationship between organs and ensuring rights and freedoms as individuals' expression.[162] On the opposite, online platforms autonomously set users' rights and organise their community without involving users which are just the product of the company and not part of that. Therefore, users' rights and freedoms are only seen as the fuel on which online platforms rely to run their business and accumulate profits. In this case, freedoms and rights enshrined in a democratic constitution compete with the discretionary private determinations which are not bound by constitutional safeguards and act like absolute power.

In this respect, the rights and freedoms in the digital environment are not just the result of a process coming from democratic participation ('bottom-up') but from the privilege granted by online platforms ('top-down'). Although online platforms base their narrative on their role in

[157] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2013).
[158] Tal Z Zarsky, 'Social Justice, Social Norms and the Governance of Social Media' (2014) 35 Pace Law Review 154
[159] David S. Evans, 'Governing Bad Behavior by Users of Multi-Sided Platforms' (2012) 27 Berkeley Technology Law Journal 1201.
[160] Tomer Shadmy, 'The New Social Contract: Facebook's Community and Our Rights' (2019) 37 Boston University International Law Journal 307, 329.
[161] Laura Stein, 'Policy and Participation on Social Media: The Cases of YouTube, Facebook, and Wikipedia' (2013) 6(3) Communication, Culture & Critique 353.
[162] Charles Howard McIlwain, *Constitutionalism: Ancient and Modern* (Amagi 2007).

establishing a global community, it is worth wondering how it is possible to agree common rules between communities which, in some cases, are also made up of two billion of people. Someone could argue that users can participate in the platforms' environment by selecting to hide news or opt-in to specific data regimes. However, it should not be forgotten that online platforms establish these possibilities leaving users a mere feeling of freedom in their digital spaces. In this regard, Jenkins distinguishes between participation and interactivity.[163] According to Jenkins, 'Interactivity refers to the ways that new technologies have been designed to be more responsive to consumer feedback' while 'Participation, on the other hand, is shaped by the cultural and social protocols'. Translating this distinction in the field of online platforms, it is possible to observe how there is no participation since online platforms autonomously define the protocols while inviting users to engage and interact. Platforms user interactivity as an alternative to participation which create a reasonable feeling of trust and involvement in online platforms' determinations.

The lack of any instrument of participation or transparency make individuals subject to the autonomous powers exercised by online platforms, leading to a process of 'democratic degradation'.[164] Therefore, it is not just a matter of formal adherence to boilerplate clauses but the lack of participation in activities which affect the rights and freedoms of billions of people in the world. This process also extends to the lack of transparency and redress mechanism. Although data protection law provides more safeguards on this point, it is possible to generally observe how online platforms avoid explaining their conducts or be accountable for the activities they perform. Within this framework, it would be possible to argue that the power exercised by online platforms mirrors, to some extent, the same discretion which an absolute power can exercise over its subjects.

4.2 The Exercise of Autonomous Powers

The relationship between platforms' powers and users is not the only piece of this authoritarian puzzle. It is also critical to understand how online platforms express different forms of power. By ToS and community guidelines, platforms unilaterally establish what users can do in their digital spaces. Platforms rely on private freedoms to regulate relationship with their online communities, precisely, determining how content and data are governed online. In the field of content, this is particularly evident. In the lack of any regulation of the process through which expression are moderated, platforms are free to set the rules according to which speech flows online. While, in the field of data, we have already underlined how, on the one hand, the GDPR introduces new safeguards and obligations, but, on the other hand, leaves the data controller broad margins of discretion in assessing the risk for data subject's fundamental rights and its ability to prove compliance with data protection principles according to the principle of accountability.

Regulating speech and data that is usually the result of legislative fights and constitutional compromises. On the opposite, online platforms autonomously set standards and procedures even if they operate transnationally and are driven by their business purposes. Put another way, these agreements compete with the traditional way individual conceives legal norms and protection as an expression of public power. From a private law perspective, these agreements can be

[163] Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York University Press 2006).
[164] Radin (n 151), 16.

considered mere boilerplate contracts, where clauses are based on standard contractual terms that are usually included in other agreements.[165] Users cannot exercise any negotiation power but, as an adhering party, may only decide whether or not to accept pre-established conditions. At first glance, the significance of this situation under a public (or rather constitutional) law perspective may not be evident, both since boilerplate contracts are very common even in the offline world and since online platforms' ToS do not seem to differ from the traditional contractual model.[166] However, how Jaffe underlined in the first half of the last century, contract law could be considered as a delegation of law-making powers to private parties.[167]

By defining the criteria according to which these decisions are enforced as well as the procedural and technical tools underpinning their ToS, platforms establish the rules governing billions of users should comply.[168] In this case, it would be possible to observe how ToS constitute the expression of a quasi-legislative power. Even if it would be possible to refer to the law of the notice provider or that established in the ToS, it is not possible to concretely assess the level of compliance with legal standards due to the lack of transparency and accountability in the online platforms' decision-making.[169] Scholars have already underlined how social media' ToS does not ensure the same degree of protection of public safeguards.[170] Although this autonomy is limited in some areas such as data protection, the global application of their services and the lack of any legal rule regulating online content moderation leave a broad margin of political discretion in their hands when drafting their ToS. In other words, similarly to the law, these private determinations can be considered as the legal basis according to which platforms exercise their powers or an expression of how platforms can promote an autopoietic set of rules which compete with the law as a social subsystem.

Besides, the exercise of quasi-legislative functions is not the only expression of platforms' power. Online platforms can enforce contractual clauses provided for in the ToS directly without the need to rely on a public mechanism such as a judicial order or the intervention of law enforcement authorities. For instance, the removal of online content or the erasure of data can be performed directly and discretionary by online platforms without the involvement of any public body ordering the infringing party to fulfil the related contractual obligations. This technological asymmetry constitutes the grounding difference from traditional boilerplates contracts. Their enforcement is strictly dependent on the role of the public authority in ensuring the respect of the rights and obligations which the parties have agreed upon. Here, the code assumes the function of the law,[171] and the network architecture shows its role as modality of regulation.[172] Platforms

[165] Woodrow Hartzog, 'Website Design as Contract' (2011) 60(6) American University Law Review 1635.
[166] Peter Zumbansen, 'The Law of Society: Governance Through Contract' (2007) 14(1) Indiana Journal of Global Legal Studies 191; Lee A Bygrave, *Internet Governance by Contract* (Oxford University Press 2015).
[167] Louis Jaffe, 'Law Making by Private Groups' (1937) 51 Harvard Law Review 201.
[168] Luca Belli and Jamila Venturini, 'Private Ordering and the Rise of Terms of Service as Cyber-Regulation' (2016) 5(4) Internet Policy Review <https://policyreview.info/node/441/pdf> accessed 16 June 2018.
[169] Paul S Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 University of Colorado Law Review 1263.
[170] Ellen Wauters, Eva Lievens and Peggy Valcke, 'Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites' (2014) 22 International Journal of Law & Information Technology 254.
[171] Lessig (n 10).
[172] Reidenberg (n 23).

can directly enforce their rights through a quasi-executive function. This private enforcement is not a novelty.[173] In the digital environment, it is the result of an asymmetrical technological position. Platforms are the rulers of their digital space since they can manage the activities which occur within their boundaries. This power, which is not delegated by public authorities but results from the network architecture itself, is of special concern from a constitutional perspective since it represents a form of self-regulation and disintermediation of the role of public actors in ensuring the enforcement of fundamental rights online.[174]

Together with these normative and executive functions, online platforms can also exercise a quasi-judicial power. Platforms have shown to perform functions which are similar to that of the judiciary and especially of constitutional courts, namely the balancing of fundamental rights. When receiving a notice from users asking for content removal or delisting, platforms assess which fundamental rights or interest should prevail in the case at issue to render a decision. Taking as an example alleged defamatory content signalled by a user, the platform could freely decide whether such content is being lawfully protected by right to inform or should protect human dignity. The same consideration applies when focusing on how the right to privacy should be balanced with freedom of expression. This is evident platforms moderate content or decide to rely on exceptions established by data protection law. These decisions are based on their business purposes without being obliged to respect or take into account fundamental rights. The result of this situation leads to chilling effect for fundamental rights and, more generally, to the establishment of a para-legal framework in the digital environment.

Furthermore, adding another layer of complexity – and concern – is the possibility that these activities can be executed by using automated decision-making technologies.[175] On the one hand, algorithms can be considered as technical instruments facilitating platform's functionalities, such as the organisation of online content and the processing of data. However, on the other hand, such technologies can constitute technical self-executing rules, obviating even the need for a human executive or judicial function. The use of automated decision-making technologies is not neutral from a constitutional law perspective. The delegation to machines of decisions involving individuals' fundamental rights involves the core of human dignity and challenges democratic values due to low degree of transparency and accountability in automated decisions.[176] The new relationship between human and machine in the algorithmic society leads to the increase of platforms' powers in deciding not only how content and data flow online but also individuals' daily life. Within this framework, there is no room for users' participation. Human and non-

[173] Rory Van Loo, 'The New Gatekeepers: Private Firms as Public Enforcers' (2020) 106 Virginia Law Review 467.
[174] Teubner (n 41); Julia Black, 'Constitutionalising Self-Regulation' (1996) 59(1) The Modern Law Review 24.
[175] Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951719897945> accessed 14 June 2020.
[176] Andrea Simoncini, 'L'algoritmo incostituzionale. Intelligenza artificiale e il futuro delle libertà' (2019) (1) Bio Law Journal 63; Frank Pasquale, *The Black Box Society. The Secret Algorithms that Control Money and Information* (Harvard University Press 2015); Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11(2) Ethics and Information Technology 105; Tal Zarsky, 'Transparent Predictions' (2013) 4 University of Illinois Law Review 1507.

human entities shape the choices of online platforms.[177] Nonetheless, the governance of decision-making is not shared but centralised and covered by unaccountable purposes. As underlined by Hartzog, Melber and Salinger, 'our rights are established through non-negotiable, one-sided and deliberately opaque 'terms of service' contracts. These documents are not designed to protect us. They are drafted by corporations, for corporations. There are few protections for the users-the lifeblood powering social media'.[178]

From a constitutional perspective, users, as members of online communities, are subject to the exercise of contractual (legitimate) authority exercised by platforms through instruments of private law mixed with technology (i.e. the law of the platforms). The three traditional public powers are centralised when focusing on platforms quasi-public function: the definition of the rules to assess online contents, the decisions over the users' complaints and their enforcement are practised by the platform without any separation of powers. Constitutionalism has primarily been based on the idea of the separation of powers, as theorised by Charles De Secondat.[179] In contrast, it is possible to highlight the rise of a private order whose characteristics do not mirror constitutional provisions but is more similar to absolute power. Precisely, this phenomenon cannot be defined as the rise of a 'private constitutional order' since neither the separation of powers nor the protection of rights are granted in this system.[180] Rather, the above-mentioned framework has shown how the absence of the separation of powers in platform activities is one of the primary reasons showing the role of private powers in the information society. This has led some authors to refer to this phenomenon as a return to feudalism,[181] or to the *ancien régime*.[182]

5. Converging Powers in the Algorithmic Society

In the last twenty years, global trends have led to the consolidation of new areas of power challenging the Westphalian model. Globalisation has contributed to the rise of metalegal system where different organisations and entities produce and shape norms with extraterritorial implications. In other words, the traditional notion of the law seems to be increasingly expanded to include the norms (auto)produced by other subsystems. This situation contributes to weakening the relationship between 'law and territory' and enhance that between 'norms and space'. The evolution of different systems leads to the emergence of different institutions which operate according to their internal rationality. As a result, the unitary of State and the role of law as a monolith of certainty is slowly replaced by the fragmentation of new institutions expressing their

[177] Ira Rubinstein and Nathan Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Technology Law Journal 1333; Robert Brendan Taylor, 'Consumer-Driven Changes to Online Form Contracts' (2011-2012) 67 NYU Annual Survey of American Law 371.

[178] Woodrow Hartzog, Ari Melber and Evan Salinger, 'Fighting Facebook: A Campaign for a People's Terms of Service' Center for Internet and Society (22 May 2013) <http://cyberlaw.stanford.edu/blog/2013/05/fighting-facebook-campaign-people%E2%809699s-terms-service> accessed 25 September 2020.

[179] Charles De Secondat, *L'esprit des loi* (1748).

[180] The French Declaration of the Rights of Man and Citizens art 16 states: 'Any society in which the guarantee of rights is not assured, nor the separation of powers determined, has no Constitution'. Declaration of the Right of Man and the Citizen, 26 August 1789.

[181] James Grimmelmann, 'Virtual World Feudalism' (2009) 118 Yale Law Journal Pocket Part 126.

[182] Belli and Venturini (n 167).

principles and values on a global scale. Such models identify roles for non-state actors, private corporations, and supranational governance institutions.

The digital environment constitutes a sort of battlefield between different systems. Different rationalities influence each other, although they develop their rules according to their rules and procedures. On the one hand, sovereign States can count on the possibility of expressing binding rules such as censorship or restriction of access to its infrastructures, also enjoying the exclusive monopoly on the use of force, on the other hand, online platforms inevitably influence the boundaries and the subjects by managing content and data on a global scale. While authoritarian states have extended their powers on the digital environment, democratic States have adopted a liberal approach entrusting online platforms with public tasks without clearly defining the boundaries of such activities or translating constitutional safeguards in their regulation. Such a transfer of responsibilities resulted from the recognition of platforms' role in establishing an effective online public regulatory framework.

Although the delegation to private actors of public tasks should not be considered a negative phenomenon per se, the lack of safeguards leaves these actors free to exercise their private sovereignty. Unlike public actors, they are not obliged to respect fundamental rights. Nonetheless, delegated powers are not the only source of concern. Platforms can indeed exercise sovereign powers over their online spaces through instruments based on contract law and technology. In the field of data and content, platforms' activities mirror the exercise of quasi-public functions contributing to define the values and the principles on which their communities are based. The discretion in setting the standard of their communities or the possibility to balance and enforce users' fundamental rights through automated systems are examples of an absolute regime resulting from a mix of constitutional freedoms and technology.

Content and data have shown to be two areas which, even if they are based on different constitutional premises, allow examining private powers online. This is not a coincidence, but it is the result of the intimate relationship between content and data in the algorithmic society. Therefore, it is time to understand the intimate relationship of content and data as well as the converge in the legal protection of these two constitutional values.

Chapter IV

From the Parallel Tracks to Overlapping Layers of Content and Data

Summary: 1. From Parallel Tracks to Overlapping Layers. – 2. An Evolving Relationship on Different Constitutional Grounds. – 3. The Intimate Connection Between Active Provider and Data Controller. – 3.1 The Blurring Lines between Content and Data. – 3.2 From Takedown of Content to Delist of Data. – 4. From Legal Divergence to Convergence. 4.1 Constitutional Conflict and Convergence of Values. 4.2 From Content to Process. 4.3 Content and Data Liability. – 5. The Challenges Ahead in the Field of Content and Data.

1. From Parallel Tracks to Overlapping Layers

The exercise of platforms powers is compelling. Delegated and autonomous powers question the role of European constitutional law in protecting fundamental rights while tackling the consolidation of powers. Nonetheless, there is still the need to focus on another layer of complexity to understand the role of digital constitutionalism in Europe, precisely the intimate relationship between the fields of content and data. Thanks to the development of new technologies, online platforms have amplified the possibility to access information and process data. The threats for freedom of expression, privacy and data protection do not come just from the rise and consolidation of platforms' powers but also are the result of the blurring boundaries of the legal regimes of expression and data in the algorithmic society.

At the end of the last century, the Union conceived the legal regimes of online intermediaries' liability for content and data in a separate way. The first area – intermediary liability – focuses on the legal responsibility of online intermediaries concerning third-party illicit actions based on the e-Commerce Directive.[1] The second field – data protection – focuses on regulating the processing of personal information according to the Data Protection Directive.[2] Both systems provide definitions, pursue specific objectives and are encapsulated by different legal instruments. For instance, whereas the Data Protection Directive could not exclude from its scope the e-Commerce Directive due to chronological reasons, the latter expressly clarified that its scope of application does not include 'questions relating to information society services covered by Directives 95/46/EC and 97/66/EC'.[3] This legal divergence shows how the Data Protection Directive and e-Commerce Directive started to run on parallel tracks from a legal point of view.

[1] 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.

[2] 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.

[3] E-Commerce Directive (n 1), Article 1(5)(b). Recital 14 defines this rigid separation by stating that: 'The protection of individuals with regard to the processing of personal data is solely governed by 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 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector which are fully applicable

This political choice perfectly makes sense in the aftermath of the Internet. At that moment, online intermediaries were predominantly performing passive activities offering access or hosting services mainly to business rather than to billions of consumers.[4] It is no by coincidence whether the relationship between content and data were not of concern for the European Commission when drafting the respective legal regimes. Online intermediaries offer services without interfering with the information they transmit and host. Therefore, the technological divergence between the field of content and data was one of the primary reasons for the legal divergence in the regulation of these fields.

In the meantime, we have experienced a process of technological convergence. Online intermediaries had become more active by offering services to share information which is indexed and organised through the processing of data.[5] Over the years, several actors have developed new services based on content and data. Together with the traditional providers of Internet access providers and hosting providers, new players have started to offer their digital services such as search engines (e.g. Google and Yahoo), platforms that allow communication, exchange and access to information (e.g. Facebook and Twitter), cloud computing services (e.g. Dropbox and Google Drive), e-commerce marketplace (e.g. e-Bay and Amazon), online payment systems (e.g. Paypal).

Online platforms can play a two-fold role based on their system of liability. On the one hand, they operate as data controllers when deciding the means and the purposes of processing personal data, but they can also be considered processors for the data they host. On the other hand, platforms actively organise users' content according to the data they collect from users even if they can rely on an exemption of liability for third-party illicit conduct. Social media are the most evident example of the intersection in between content and data. The moderation of content and the processing of data is not performed by chance. Expressions are moderated with the precise scope of ensuring peaceful environment where users can share their ideas and opinions, thus, allowing platforms to collect data from offering micro-targeting advertising services.[6] Likewise, search engines organise their content according to billions of search results for providing the best targeted services attracting advertising revenues. These examples do not exhaust the way in which content and data are increasingly converging from a technological perspective, but they can lead to defining the relationship between content and data as intimate.

This framework inevitably affects the legal regimes of content and data as far as platforms' liability is concerned. Despite the original parallel track, content and data have started to overlap

---

to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States'. However, the same Recital does not exclude that 'the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet'.

[4] Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017).

[5] Giovanni Sartor, 'Providers Liability. From the eCommerce Directive to the Future' (2017) In-depth analysis for the IMCO Committee <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf> accessed 2 December 2018.

[6] Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).

not only from a technological but also legal standpoint. The blurred lines in the field of content and data is not a neutral phenomenon from a constitutional law perspective. A silos approach in the field of content and data has raised several challenges for the protection of legal certainty as well as some of the most important fundamental rights in the information society: freedom of expression, privacy and data protection. Within the framework of the Digital Single Market strategy, the Union has introduced new legal instruments indirectly making the fields of content and data closer and leading to legal convergence. In other words, the shift from parallel tracks to overlapping layers (or the move from technological and legal divergence to convergence) is a crucial piece of the puzzle to understand the framework in which platforms exercise their powers and shape democratic values.

Within this framework, this chapter aims to analyse the evolving technological and legal intersection between the legal systems of content and data. The primary goal is to explain how the rise of platforms powers is also linked to the blurring connection between these two (legal) fields. Understanding to what extent the two regimes have started to converge in the algorithmic society is critical when addressing platforms' functions. The first part examines the points of convergence and divergence between the legal regimes introduced by the e-Commerce Directive and the Data Protection Directive. In the second part, their evolving relationship is contextualised in the framework of the information society by providing two examples of judicial interpretation showing how technological convergence has led to overlapping layers between the two legal fields which were conceived on parallel tracks. The third part examines the role of European digital constitutionalism in answering technological with legal convergence. Firstly, this part underlines how the first type of legal convergence occurred at the constitutional level as a reaction against the risk of technological convergence in the field of content and data. Secondly, this part underlines the shift from substantial to procedural rules to foster transparency and accountability in the field of content which is increasingly moving towards rules and procedures characterising data protection. The third path of convergence looks at the evolution of online intermediaries' liability in the field of content and data.

2. An Evolving Relationship on Different Constitutional Grounds

At the end of the last century, the Union could not foresee how content and data would have started to become increasingly interrelated. If someone looks at the Internet when the liability regimes of content and data saw the light, it would be likely to find a digital world without social media platforms, e-commerce marketplaces and other digital services. The role of intermediaries was merely passive offering storing, access and transmission of data across the network.

Within this framework, the Data Protection Directive was adopted in 1995 with the aim to ensure the free flow of personal data from one Member State to another. Only five years later, the e-Commerce Directive entered into force to ensure the free movement of information society services. The two legal instruments share the common intent to foster the development of the internal market and (also) protect two constitutional sets of values, especially shaped by the framework of the Council of Europe at that time through the rights enshrined in the European Convention on Human Rights ('Convention'). On the one hand, the Data Protection Directive focused on the right to privacy and protection of personal data. On the other hand, the e-commerce Directive was concerned with the protection of the right to freedom of expression.

Although freedom of expression, privacy and data protection are protected as fundamental rights, nevertheless, their rise and consolidation in the European framework have not the same constitutional history. When dealing with freedom of expression in Europe, it is possible to look at such fundamental right in at least through three different perspectives. Freedom of expression is enshrined in the Charter and in the Convention as well as in each Constitution of Member States.[7] The predominance of freedom of expression in the Europe finds its roots in the French Declaration of the Rights of Man and of the Citizen protecting 'the free communication of thoughts and of opinions'.[8] Since the XIX century, freedom of expression has been developed as an answer to the political power exercised by public authorities and then was the basis for protecting other rights such as the right to education and research.

Instead, the European path towards the constitutional recognition of privacy and data protection as fundamental rights started from the evolution of the concept of privacy in the US framework.[9] From a merely negative perspective, the right to be left alone, characterised by predominant liberal imprinting, the right to privacy has firstly emerged in Europe within the framework of the Convention. As we will see in Chapter VI, this liberty has then evolved towards a positive dimension consisting in the right to the protection of personal data as an answer to the progress of the welfare state and development of new automated processing techniques like databases.[10] Data protection in the European framework constitutes a relatively new individual right developed as a response to the rise of the information society driven by new automated technologies and, primarily, the Internet. In other words, if the right to privacy was enough to meet the interests of individuals' protection, in the information society, the widespread processing of personal data, also through automated means, has made no longer sufficient to protect only the negative dimension of the aforementioned fundamental right.

Both the e-Commerce Directive and the Data Protection Directive was adopted to face the challenges of new information technologies for the internal market.[11] As underlined in Chapter II, the Union was more concerned to focus on ensuring the smooth development of the internal market by pursuing a digital liberal approach. To ensure this goal, the Union underlined the need to protect fundamental values. On the one hand, the Data Protection Directive identifies the right to privacy and data protection as the beacon to follow to 'contribute to economic and social progress, trade expansion and the well-being of individuals',[12] whereas, the e-Commerce Directive protects freedom of expression since 'the free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely

[7] Eric Barendt, *Freedom of Speech* (Oxford University Press 2017).
[8] French Declaration of the Rights of Man and of the Citizen (1789), Art 11.
[9] Samuel D. Warren and Louis D. Brandeis, 'The right to privacy*'* (1890) 4 Harvard Law Review 193.
[10] Alan F. Westin, *Privacy and Freedom* (Atheneum 1967).
[11] Data Protection Directive (n 1), Recital 4. Moreover, Recital 14 states that 'given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data'. E-Commerce Directive (n 1), Recital 1. 'The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples'.
[12] Data Protection Directive (n 1), Recital 2.

freedom of expression'.[13] As a result, the two legal regimes have been conceived with a clear political perspective: ensuring the smooth development of the internal market by providing new rules and adapting fundamental freedoms to the new technological scenario.

These constitutional observations do not exhaust the relationship between the two systems. The parallel track in the online platforms' liability is also based on other grounding differences between the two regimes. The e-Commerce Directive focuses on content rather than procedures, while the Data Protection Directive follows the opposite path. The regime of content is based on the removal of unlawful speech but not how this procedure occurs. On the opposite, European data protection law does not focus on prohibiting the processing of personal data but tackling the unlawful processing. In other words, the two regimes have been built on parallel tracks characterised by different focal points. On the one hand, the content regime under the e-Commerce Directive is based on secondary liability for third-party illegal content or behaviours. On the other hand, the Data Protection Directive has introduced a system of liability of the controller independent from third-party conducts.

However, even these considerations are just a small part of the jigsaw. When focusing on the liability regime system of the two legal instruments, some scholars observed that the two regimes should not be considered as mutually exclusionary but needs to be understood beyond a literal interpretation.[14] Precisely, before the adoption of the e-Commerce Directive, the Commission recognised the horizontal nature of online intermediaries' liability involving 'copyright, consumer protection, trademarks, misleading advertising, protection of personal data, product liability, obscene content, hate speech, etc.'.[15] Even after its adoption in 2000, the Commission stressed the general scope of the e-Commerce Directive in relation to third-party content.[16] Besides, the e-Commerce Directive would provide another clue when it specifies that different civil and criminal liability regime of liability at domestic level could negatively affect the internal market.[17] This interpretative provision could be understood as a goal towards harmonisation of the liability systems covering any type of online content to reduce legal fragmentation which would undermine the development of the internal market.

Within this framework, there are at least three types of cases where the regime of content and data would apply.[18] First, when users commit an infringement through online intermediaries' networks (e.g. defamation), the e-Commerce Directive applies, thus, shielding the liability of online platforms. Therefore, online platforms are not liable provided that they remove the infringing content if they become aware of the users' illicit conduct. Second, when users infringe

[13] E-Commerce Directive (n 1), Recital 9.
[14] Mario Viola de Azevedo Cunha and others, 'Peer-to-peer Privacy Violations and ISP liability: Data Protection in the User-generated Web' (2012) 2(2) International Data Privacy Law 50.
[15] Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157 C4-0297/97), 203.
[16] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), COM(2003) 702 final.
[17] E-Commerce Directive (n 1), Recital 40.
[18] Bart van der Sloot, 'Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe' (2015) 3 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 211.

privacy and data protection rules through online intermediaries' networks, the Data Protection Directive applies. In this case, platforms are liable just for primary infringements of data protection rules and not for users' illicit conducts. Third, where users infringe a right falling outside the scope of data protection rules (e.g. hate speech) and platforms are required to provide details about the infringing users (i.e. personal data) or to implement filtering systems, both the e-Commerce Directive and the Data Protection Directive applies.

In the last case, it is possible to find a first (but indirect) point of contact between the two regimes. More specifically, in *Promusicae*,[19] a collecting society representing producers and publishers of musical and audiovisual recordings, asked Telefonica, as access provider, to reveal personal data about its users due to alleged access to the IP-protected work of the collecting society's clients without authors' prior authorisation. The question referred to the ECJ was directed to understand if an access provider could be obliged to provide such information to the collecting society according to the legal framework provided for by Directive 2004/48/EC ('Enforcement Directive'),[20] Directive 2001/29/EC ('Infosoc Directive'),[21] and Directive 2002/58/EC ('e-Privacy Directive').[22] The ECJ found that Member States are not required to lay down an obligation requiring intermediaries to share personal data to ensure effective protection of copyright in the context of civil proceedings. It is for Member States to strike a fair balance between the rights at issue and take care to apply general principles of proportionality. However, even in this case, although the system of content and data (in this case, the e-Privacy Directive) participated in the same reasoning of the ECJ, it was not clear the mutual influence of the two regimes at that time.

Likewise, in *LSG*,[23] the ECJ recognised that the rules of the Enforcement Directive, the Infosoc Directive and the e-Privacy Directive, do not prevent Member States from establishing a reporting obligation for online intermediaries concerning third parties traffic data in order to allow civil proceedings to commence for violations of copyright. Even in this case, the ECJ has specified that such a system is compatible with Union law provided that Member States ensure a fair balance between the different fundamental rights at stake. The same orientation was confirmed in *Bonnier Audio*,[24] where the ECJ stated that EU law does not prevent the application of national legislation which, in order to identify an internet subscriber or user, allow in civil proceedings to order an online intermediary to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement.

---

[19] Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU (2008).
[20] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (2004) OJ L 195/16.
[21] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) OJ L 167/1.
[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L 201/37.
[23] Case C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH (2009).
[24] Case C-461/10 Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB (2012).

Although these cases could provide a first overview of a primordial legal overlap between the regimes of data and content, both systems remained formally far from each other. In this phase, the relationship between data and content was still limited to sharing of personal data concerning third-party infringements. In other words, this phase was still characterised by technological and legal divergence in the field of content and data. These considerations do not still provide significant grounds for understanding how and why the two regimes have started to overlap. The parallel tracks in the legal regime of content and data are not just the result of the adoption of two different legal instruments but it is also the result of a different technological environment at the end of the last century. However, the next section examines the technological convergence leading towards the legal convergence in the field of content and data.

3. The Intimate Connection Between Active Provider and Data Controller

Online platforms are complex creature. From the data perspective, they decide how to process vast amounts of data coming from users' information and content for profit. Concerning expressions, they actively moderate content to attract users and their information. The blurring lines between content and data in the online platforms' environment challenges the two systems based on parallel legal regimes.

The overlap between content and data started to be clear to the ECJ when, in *Google France*,[25] it observed that Google on the one hand, 'processes the data entered by advertisers and the resulting display of the ads is made under conditions which Google controls'.[26] The court, then observed, that this activity does not deprive Google of the exemptions from liability provided for in the e-Commerce Directive. Likewise, in the *L'Oreal* case,[27] the court did not follow the aforementioned path, recognising, instead, that eBay processes the data entered by its customer-sellers. Besides, according to the Luxembourg judges, '[w]here […] the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31'.[28] In these cases, the ECJ identified a connection between the data processed by the platform and its active role in relation to the exemption of liability. At that time, we were still at the beginning of the rise of platforms' powers in the digital environment. The consolidation of parallel tracks in the field of data and content is still the result of those legal regimes which now clash with the reality of the algorithmic society. The constitutional gap was still reflected in the provisions of the two legal regimes which did not provide bridges between legal fields.

In the framework of content, online intermediaries are defined as entities offering access, caching or hosting services whose activity is exempted from secondary liability due to their

[25] Joined cases C-236/08 to C-238/08 Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08) (2010).
[26] Ibid, 115.
[27] Case C-324/09 L'Oréal SA and Others v eBay International AG and Others (2011).
[28] Ibid, 116.

passive nature.[29] Firstly, access providers (or *mere conduit*) are defined as services consisting of the transmission in a communication network of information provided by a recipient of the service.[30] Secondly, caching providers perform services bases on the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request.[31] Thirdly, hosting providers store information provided by a recipient of the service.[32]

These providers are shielded from liability due to the technical operations they perform. They can be liable when they start to play a more active role showing awareness of the content they host. In other words, the more providers perform their activities in an active way (e.g. creating content), the more they could be subject to liability. Access providers are not responsible provided that they do not initiate the transmission, select the receiver of the transmission, select or modify the information contained in the transmission.[33] Without focusing on caching provider,[34] hosting providers are not liable for the information stored in their digital spaces provided that two alternative conditions are satisfied. Firstly, online intermediaries are not liable when they have not actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent. Secondly, the exemption of liability also covers the case when online intermediaries, upon obtaining such knowledge or awareness, act expeditiously to remove or to disable access to the information.[35]

While there are no issues in considering Vodafone or Verizon as access providers and Facebook or Twitter as hosting providers, the situation is more complicated when focusing on search engines like Google (i.e. information location tool services). The definition of 'information society service' would cover their activities.[36] Nonetheless, it is not entirely clear if search engines fall under any of the three types of services providers mentioned above. It is not by chance whether the e-Commerce Directive clarifies that 'In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services', thus, leaving Member States this choice.[37]

---

[29] E-Commerce Directive (n 1), Recital 42. 'The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'.

[30] Ibid, Art 12.

[31] Ibid, Art 13.

[32] Ibid, Art 14.

[33] Ibid, Art 12(1)(a-c).

[34] Ibid, Art 13(1)(a-e).

[35] Ibid, Art 14(1)(a-b).

[36] Ibid. According to Recital 18: '[I]nformation society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data'.

[37] Ibid, Art 21. The reasons for such a choice came from the passive activity of search engines which do not take editorial decisions over content. They are not either the source of information they index or able to remove this information online. For instance, Some Member States (e.g. Portugal and Spain) have considered search engine services as hosting providers. See Joris van Hoboken, 'Legal Space for Innovative

Moving to the field of data, the Data Protection Directive adopts a different approach. It does not exempt from liability online intermediaries according to their passive roles but provide a comprehensive definition of data controllership.[38] 'Data controller' is indeed defined as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.[39] Within this framework, the data controller can be defined as the governor of personal data since it can exercise a form of decision-making.[40] This power consists of the possibility to select the 'purposes and means', thus, subjecting data subject's personal data to the purposes and goal of the data controller.[41]

Unlike in the field of content, this definition reflects an active engagement rather than a passive and technical role. Online intermediaries falling within this definition would be in charge of the governance of the processing of personal data of their businesses. In other words, these definitions reflect the lack of a common starting point between the two regimes. On the one hand, as far as the legal regime of content is concerned, online intermediaries are depicted as passive entities responsible only when they perform activities as content providers. Whereas, data controllers are the key players of the data protection system since they actively define the modalities according to which data is processed.

The data controller is not the only relevant figure in the field of data. The Data Protection Directive also provides the definition of 'processor', which is the 'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.[42] It is evident how the role of data processors is subject to the data controllers' guidelines and, therefore, its role can be defined passive rather than active. In other words, the data controller is the brain of data governance, the processor is the brawn. The definition of data processor fits with purely passive providers, that neither determine the means nor the purpose of the data processing. According to the WP29: 'An ISP providing hosting services is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If, however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing'.[43] Put another way, when online intermediaries only process data of third-party services such as hosting a specific website, they operate as mere passive providers and data processor. Whereas, when the

---

Ordering: On the Need to Update Selection Intermediary Liability in the EU' (2009) 13 International Journal of Communication Law & Policy 1.

[38] The ECJ has shown how much this definition could be interpreted broadly. See Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (2018).

[39] Data Protection Directive (n 1), Art 2(d).

[40] Brendan Van Alsenoy, 'Allocating Responsibility Among Controllers, Processors, And "Everything In Between": The Definition of Actors and Roles in Directive 95/46' (2012) 28 Computer Law & Security Review 30.

[41] It is worth mentioning that this situation become more intricate when data controllership is exercised by more than one entity. In this case, two or more actors govern the processing of personal data and, therefore, determining which entity is in control or responsible could be not an easy question to answer.

[42] Ibid, Art 2(e).

[43] Working Party Article 29, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf> accessed 18 June 2020.

data is processed for the purposes and according to the modalities defined by online intermediaries, this actor plays the role of active providers and data controller.

As Erdos underlined, it is possible to identify '(i) those that are not only intermediary "hosts" but also only data protection "processors" (labelled "processor hosts"), (ii) those which are intermediary "hosts" but also data protection "controllers" (labelled "controller hosts") and (iii) those which are data protection 'controllers' and not intermediary "hosts" (labelled "independent intermediaries")'.[44] While the exemption of liability for online intermediaries was introduced to protect entities by virtue of their passive role, nowadays, the use of automated systems of filtering and processing preferences have led these entities to perform activities whose passive nature is hard to support. As a result, nowadays, some online intermediaries perform no longer a merely passive role, but they are increasingly involved in active tasks. Therefore, the old-school rules in the framework of online intermediaries could not fit in the algorithmic society where online platforms actively run their business at the intersection between content and data.

While mere hosting services would fall under the first category (passive provider/data processor), online platforms, such as social networks and search engines, are likely to fall under the second relationship (active providers/data controllers). This shift should not surprise since, as we have examined in Chapter III, online platforms' activities are usually performed for profit resulting from advertising revenues based on profiling users' data. In order to manage their online space and profile users, platforms rely on automated decision technologies to organise online content and processing data. The role of platforms' in the organisations of content and profiling of users' preferences by using artificial intelligence technologies has transformed the role of online intermediaries from passive providers and data processor in active providers and data controllers. Passive hosting providers such as web service application does not choose how to process large amount of data, but they limit to offer hosting services for digital services playing the role of data processor.

These considerations are the grounding reasons to understand how online platforms play a double role of hosting providers and data controller in the algorithmic society. This situation is the primary example of the technological convergence between the two fields which has been characterised by legal divergence since the end of the last century. The following subsections examine the evolution of this relationship by focusing on two landmark cases showing how technological convergence has challenged the legal regime of content and data, thus, paving the way towards a new overlapping relationship overcoming parallel tracks.

3.1 The Blurring Lines between Content and Data

Moving to the Italian framework, the *Google v Vivi Down* saga provides clues to understand the evolution of the relationship between content and data.[45] The case raised from a video showing

[44] David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' (2018) 26 International Journal of Law and Information Technology 189, 192.

[45] It is worth mentioning that this case is not the only example of how Member States have interpreted the intersection between the fields of content and data in the last years. Nevertheless, the Italian saga allows to deal with the core of this chapter. See Erdos (n 44).

an autistic boy being bullied by his classmates uploaded to the Google video platform.[46] This situation involved both the field of content and data since the video uploaded the content on Google Video is the content in question while particular categories of personal data (i.e. health data) are processed through the hosting of the video in question. It is not by chance if the charges concerned the failure to prevent the crime of defamation against the minor and the association according to Articles 40 and 595 of the Italian criminal code (i.e. content) as well as the unlawful processing of personal data according to Article 167 of Legislative Decree 196/2003 (i.e. data).

The Court of Milan acquitted the defendants from the crime of defamation, excluding that Google, as hosting provider, had an obligation to prevent crimes committed by its users.[47] Indeed, Legislative Decree 70/2003, implementing the e-Commerce Directive in the Italian legal order, excludes the obligation to monitor content disseminated by users. Instead, the Court of Milan instance condemned three executives from Google for the crime of unlawful processing of personal data sentencing them to a six-month suspended conviction. According to the court, Google should have warned the uploaders about the obligations to respect when uploading online contents as well as the consequences of potential violations.

The Milan Court of Appeals overturned the 2010 first instance ruling by finding the Google executives were not guilty of unlawful data processing.[48] Therefore, Google would not be responsible for defamation and unlawful processing of personal data. The appeal decision was based on the general principle that Google was not aware of the content since it has no general duty to monitor user-uploaded content on their systems. Besides, the search engine could not be considered a data controller. Service providers are wholly extraneous in relation to the information stored when the e-Commerce Directive was introduced. According to the court, this figure would appear to have been overtaken in practice, however, as a result of the way in which the worldwide computer network has evolved. In today's world, the services that online intermediaries offer are not limited to the technical process that simply sets up and provides access to the network: they extend to make it possible for users to submit their own content and other people's content on the network and they cannot escape from the complying with data protection law. By recalling the decision of the court of first instance, the court observed that the active hosting providers would be subject to more onerous duties than passive hosting providers. This extension of duties would come from the organisation and selection of information. Data processing would then make online intermediaries aware of the indistinct flow of data. Nevertheless, the court clarified that this situation does not lead to a sort of chain reaction resulting

[46] See Oreste Pollicino and Ernesto Apa, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective* (Egea 2013); Giovanni Sartor & Mario Viola de Azevedo Cunha, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) International Journal of Law & Information Technologies 15; Raul Mendez, 'Google case in Italy' (2011) 1(2) International Data Privacy Law 137.

[47] Court of Milan, decision no. 1972/2010. Alessandro Mantelero, 'La responsabilità on-line: il controllo nella prospettiva dell'impresa' (2010) (3) Diritto dell'informazione e dell'informatica 405; Carmelo Rossello, 'Riflessioni de jure condendo in materia di responsabilità del provider' (2010) (4-5) Diritto dell'informazione e dell'informatica 617; Giovanni Sartor and Mario Viola De Azevedo Cunha, 'Il caso Google-Vividown tra protezione dei dati e liberta di espressione on-line' (2010) (4-5) Diritto dell'informazione e dell'informatica 645; Francesco Di Ciommo, 'Programmi-filtro e criteri di imputazione/ esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down' (2010) (6) Diritto dell'informazione e dell'informatica 829; Giovanni M. Riccio, 'Social networks e responsabilità civile' (2010) (6) Diritto dell'informazione e dell'informatica 859.

[48] Court of Appeals of Milan, decision no. 8611/2013.

in an extension of online intermediaries' liability for whatever third-party offences relating to the communication and upload of particular categories of data. In this case, the court argued that Google could not be considered a data controller.

The mix of these observations reflects how the layers of content and data tend to overlap. In this case, the matter involves data protection since it concerns the assessment of the crime of unlawful data protection, so that the Data Protection Directive applies. As a result, Google could not rely on the exemption of liability since these rules are enshrined in a separate legal instrument whose cope of application does not extend to matters involving data protection. Nevertheless, the Milan Court of Appeals mixed the two systems in its reasoning with the result that the boundaries between the two regimes started to become increasingly blurred.

The Italian Supreme Court, upholding the decision of the Milan Court of Appeals, clarified the boundaries of the previous decision in relation to the qualification of the hosting providers as data controller.[49] The Supreme Court dismissed the appeal of the public prosecutor confirming that hosting providers are not required to generally monitor data entered by third parties on its digital rooms. According to the court, although the illegal processing of personal data occurred, as the video actually contained health data of the minor, this criminal conduct is attributable only to the uploader. The hosting provider was not aware of the illicit content and, as soon as the authority notified the provider, the content was promptly removed from the online platform.

In this case, the Supreme Court has expressly addressed the topic of the coordination between the regime of the online intermediaries' liability and data protection, as implemented in the Italian legal order respectively by Legislative Decree 70/2003 and 196/2003. The court observed that the exclusion of data protection from the scope of application of the Legislative Decree 70/2003 clarifies that the protection of personal data is governed by rules outside the scope of online intermediaries' liability for hosting third-party content. Therefore, the two regimes should be interpreted together meaning that the online intermediaries' liability regime helps to clarify and confirm the scope of the data protection regime. The role of the data controller implies the existence of decision-making power with regard to the purposes, the methods of processing personal data and the tools used. Put another way, the data controller is the only subject who can determine its aims, methods and means. In the view of the Supreme Court, this role is compatible with the system of the e-Commerce Directive. Precisely, the court observed that as long as the illicit data is unknown to the service provider, this entity cannot be considered as the data controller, because it lacks any decision-making power on the data itself. When, instead, the provider is aware of the illicit data and does not take action for its immediate removal or to make it inaccessible in any case, it fully assumes the status of data controller.

The decision of the Supreme Court was based on a mix between the legal regimes of content and data. Even more importantly, this observation underlines a critical evolution of the role of online intermediaries whose neutral functions turned into a more active involvement characterised by the determination of the scope and purposes for processing personal data.

[49] Italian Supreme Court, decision no. 5107/2014.

3.2 From Takedown of Content to Delist of Data

The judicial activism of the ECJ has contributed to indirectly underlining how the regimes of content and data would have been destined to overlap in the framework of the algorithmic society. The *Google Spain* case is a landmark decision for several reasons but, for the purpose of this chapter, it is a clear example of convergence between the regimes of content and data.[50]

Without going back on the facts of the case and on the primary legal issues already underlined in previous chapter and by several works,[51] it is interesting to underline how, although the Google Spain case focused on data protection law, it shares similarities with the field of content. Like in the framework of the e-Commerce Directive, the case concerns the removal (*rectius* delisting) of online content including personal data. This action would have triggered the responsibility of the search engine as hosting provider under Spanish law to remove the content at stake. In the *Google Spain* case, however, the matter was addressed from the data perspective.

This case still shows a high degree of convergence. The opinion of the Advocate General Jääskinen provides interesting clues, precisely, when he firstly rejected the idea of search engines as data controllers.[52] This conclusion came from the interpretation of the notion of data controller based on the idea of 'responsibility' over the personal data processed 'in the sense that the controller is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing as personal data'.[53] This last view circularly brings back to the argument of the Italian Supreme Court when underlining the link between the notion of data controller and its responsibility in terms of awareness. This argument highlights the potential merge of the field of content and data where awareness seems a condition for identifying controllership. In other words, the responsibility of the data controller would result from its awareness about what it is doing when processes personal data like for online intermediaries in the field of content. According to the Advocate General, 'the internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party web pages. The service provider is not aware of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way'.[54]

The Advocate General did not exclude that upon certain conditions even a search engine does exercise control on personal data and may therefore be subject to the obligations set forth under the Data Protection Directive in its capacity as data controller. The owner of a search engine has

[50] Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014).
[51] See Aleksandra Kuczerawy and Jef Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Columbia Technology Law Journal 219; Frank Pasquale, 'Reforming the Law of Reputation' (2015) 47 Loyola University of Chicago Law Journal 515; Oreste Pollicino and Marco Bassini, 'Reconciling Right to be Forgotten and Freedom of Information in the Digital Age. Past and Future of Personal Data Protection in the EU' (2014) 2 Diritto pubblico comparato ed europeo 641.
[52] Opinion of the Advocate General Jääskinen in the case Google Spain C-131/12, 25 June 2013.
[53] Ibid, 82.
[54] Ibid, 84.

control over the index and can filter or block certain content.[55] A search engine can be required to apply exclusion codes on source pages to prevent the retrieval of specific content. Even with respect to the cache copy of the content of websites, in case of request of updating the same by the owner, the search engine has actual control over personal data.[56]

The assumption behind this finding would be based on considering the liability of search engines dependent on their active role based on its awareness. In light of that, the opinion reached the conclusion that Google could not be considered a data controller.[57] The conclusion of the Advocate General shows how the two legal regimes inevitably overlap. The assessment about whether a search engine can be considered a data controller has been based on legal arguments resembling the framework of the e-Commerce Directive. In other words, the impossibility to control personal data in the case of delisting was connected to a passive role incompatible with data controllership.

Focusing on the ECJ's decision, even though the court has agreed that the indexing of information retrieved from third parties' websites amounts to a processing of personal data, this point has remained the only common finding between the opinion of the Advocate General and the decision of the court. As far as the divergence between the two approaches is concerned, it is when answering the question as to the nature of the search engine as data controller that the court takes an opposite path. The ECJ's decision firmly recognised that search engines are data controllers, especially these actors play a decisive role 'in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published'.[58] Therefore, the ECJ abandoned the idea of awareness and responsibilities advanced by the Advocate General and focused on the current effects of the search engines' activities. Put another way, the court dismantled any potential convergence going back to parallel tracks.

A critical point lies with the court's observation that excluding search engines from the notion of data controller would be contrary to the objective of the provision, which is to ensure effective and complete protection of data subjects. The assumption behind this reasoning in this respect seems to be that ensuring higher protection of data subjects requires taking a broader definition of data controller. This consideration is also explained by the interest of the ECJ to ensure effective protection of the right to privacy as underlined in Chapter II. The finding of the court in *Google Spain* does not seem to be supported by the actual manner search engines act when indexing third parties webpages, but rather by the crucial implications that said activity produces with regard to the protection of personal data. The argument advanced by the Advocate General, according to which an online intermediary qualifies as data controller only upon certain conditions, is thus rejected: the search engine provider amounts to a data controller regardless of the fact that the owner of a website has chosen to implement exclusion protocols or taken other arrangements for excluding the content of the same from being retrieved. The fact that the owner of a website does not indicate so, in the view of the court, does not release the search engine from its responsibility for the processing of personal data carried out as such. It cannot be excluded that

[55] Ibid, 92.
[56] Ibid, 93.
[57] Ibid, 100.
[58] C-131/12 (n 50), 36, 37-40.

defining search engines as data controller would be incompatible with data protection law since these actors would not be able to comply with all the obligations applying to data controllers.[59] It is worth underlining that, when recognising Google as data controller, the ECJ has underlined that such role should be carried out 'within the framework of its responsibilities, powers and capabilities', thus, providing a safety valve against the disproportionate extension of data protection law obligations to search engines.[60]

Although this part of the decision would show the lack of intention to reduce the gap between the legal regimes of content and data, an example of the blurring line between the two fields comes from the paragraphs of the decisions where the ECJ supported the right to delist by interpreting the provisions of the Data Protection Directive.[61] The ruling of the ECJ raises several questions on the legal regime of search engines in the field of data and content. The primary question is whether search engines' results have not been considered like third-party content since they are generated from content providers like users and hosted by search engines as service providers. It is true that the ECJ was called to answer the questions raised by the national judge through the preliminary reference mechanism focused on data protection law. Nonetheless, since the right to delist has been clustered within the framework of personal data, the application of the e-Commerce Directive is not under discussion. The Google Spain decision did not refer to the legal framework of the e-Commerce Directive. The ECJ just focused on whether Google should be considered subject to European data protection law and its obligations without thinking about the consequences for the moderation of third-party content subject to delisting. Without knowing that, the ECJ built an important bridge between the fields of content and data.

The exclusive focus on data protection law does not mean that the decision had not produced substantial effects on the regime of liability in the field of content. The ruling indeed led to the creation of new complaint-based system mirroring the notice-and-takedown system established by the e-Commerce Directive.[62] From a broader perspective, the decision affects the framework of liability of search engines. Despite the high level of protection to fundamental rights, the ECJ has also delegated to search engines the task of balancing fundamental rights when assessing users' request to delist online content. The right to delist provides a broader remedy than the obligation to remove required to online platforms in case of awareness of illicit content. Search engines are required to assess users' requests which should not be based on alleged illicit content but on their personal data. Therefore, platforms can exercise their discretion in deciding whether proceeding with the delisting, so that, in this case, search engines performs a 'data moderation' rather a 'content moderation'.

Both procedures of takedowns are not identical but similar. The notice-and-takedown mechanism was introduced in the field of content not only as the result of the liability exemption to online intermediaries but also to incentivise these actors to keep clean their spaces from illegal

[59] Miquel Peguera, 'The Shaky Ground of the Right to Be Delisted' (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 507.
[60] C-131/12 (n 50), 38.
[61] Data Protection Directive (n 1), Arts 12(b), 14(a).
[62] Stavroula Karapapa and Maurizio Borghi, 'Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm' (2015) 23 International Journal of Law & Information Technology 261.

content online.[63] The 'notice and takedown' and the 'notice and delist' are different, especially since they come from two different legal frameworks. Notice-and-takedown aims to tackle illegal third-party content while, in the field of data, notice-and-delist deals with legal content linked by the search engines' activities. The former mainly concerns the liability for third-party behaviours while the latter focuses on platforms' primary misconducts.

Besides, both procedures affect content. Even if, at first glance, the right to delist would address the removal of links to publication including personal data, however, such an activity is highly dependent on the content in question due to the balancing between data protection and freedom of expression. The effects on the users' rights to freedom of expression are similar and, therefore, there is no much difference between the two systems even if they have been based on two different legal tracks. It is no by chance if Keller underlined that the case of the right to be forgotten online looks like 'a textbook intermediary liability law'.[64] Even more importantly, failing to comply with these systems upon receiving users' notice would lead search engines to be liable. The fact that engines are data controller would mean that they can exercise a sort of control over information and, particularly, on personal data. This situation seems to be in contrast with the ban of general monitoring obligation established by the e-Commerce Directive. In other words, this decision moves the notice-and-takedown approach from the field of content to data without assessing the technological and legal boundaries between the two regimes.

4. From Legal Divergence to Convergence

The regimes of content and data have already shown a certain degree of technological convergence in the digital environment. While the relationship data processor/passive provider such as in the case of web hosting does not raise particular issues, the second model (data controller/active provider) questions the separation of the two regimes.

Despite the increasing connection between content and data, at first glance, this intersection has not led the Union to adopt a new approach to platforms liability in the framework of the algorithmic society. In the field of content, the Union has introduced new rules addressing the intersection between content and data.[65] A parallel track approach is still primary when looking at the Directive on Copyright in the Digital Single Market ('Copyright Directive'),[66] and the

[63] OECD, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives' (2011) <http://www.oecd.org/internet/ieconomy/48685066.pdf> accessed 10 February 2020.
[64] Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation' (2018) 33 Berkley Technology Law Journal 297, 354.
[65] Several European legal instruments provide a specific legal framework in respect of specific types of illegal contents online. In particular, Directive 2011/93/EU requires Member States to take measures to remove web pages containing or disseminating child pornography and allows them to block access to such web pages, subject to certain safeguards. Directive (EU) 2017/541 regards online content removal in respect of online content constituting public provocation to commit a terrorist offence. It should not be forgetting also Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, it is possible for competent judicial authorities to issue injunctions against intermediaries whose services are being used by a third party to infringe an intellectual property right.
[66] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130/92.

amendments in the framework of the Audiovisual Media Service Directive ('AVMS Directive').[67] Similarly, the GDPR as well as the Proposal for a Regulation on Privacy and Electronic Communications,[68] governs privacy and data protection law. Although a new phase of European digital constitutionalism raised within the framework of the Digital Single Market strategy, this connection does not imply the Union approach can be considered coherent with the intertwined challenges in the field of expressions and data. Within this framework, in *La Quadrature du Net*,[69] the ECJ addressed a case concerning the intersection between the legal regimes of content and data. The case concerned the lawfulness of Member States' legislation, laying down an obligation for providers of electronic communications services to forward users' traffic data and location data to a public authority or to retain such data in a general or indiscriminate way. The ECJ confirmed that EU law precludes this form of surveillance, precisely, the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security.[70] For the purposes of understanding the relationship between content and data, it is worth stressing that the ECJ observed that the protection of the confidentiality of communications and of natural persons with regard to the processing of personal data in the context of information society services are governed only by European data protection law.[71] The court has not only underlined that this field falls within the field of data but also that 'the protection that Directive 2000/31 is intended to ensure cannot, in any event, undermine the requirements under Directive 2002/58 and Regulation 2016/679'.[72]

Notwithstanding the parallel tracks approach seems predominant from this formal perspective, the substantive margins of convergence between the field of content and data underline a trend toward legal convergence. A closer focus can reveal that, despite the fragmentation of the Digital Single Market strategy, the characteristics of European digital constitutionalism provides a perspective to underline the legal convergence between content and data. The convergence between these two systems can be analysed from at least three perspectives described in the next subparagraphs. Firstly, paths of convergence between content and data in the platforms' environment are the result of the relationship between freedom of expression and data protection at the constitutional level. If, on the one hand, these two fundamental rights have led to parallel

[67] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018) OJ L 303/69.
[68] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L 119/1; Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.
[69] Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier ministre and Others (2020).
[70] See also Case C-207/16 Ministerio Fiscal (2018); Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (2016); Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (2014).
[71] Joined Cases C-511/18, C-512/18 and C-520/18 (n 69), 199.
[72] Ibid 200.

legal regimes, on the other hand, they pursue the same constitutional mission to protect democratic values. Freedom of expression and data protection does not only share the same rank of constitutional rights, but their degree of protection has also led the Union to enter into a new constitutional phase. Secondly, the regime of content is increasingly approaching the system of data. The Union has partially focused its attention on regulating the procedures on which content are processed without dealing with their legal qualification. In other words, the shift from substantial to procedural rules in the field of content resembles the rules and procedures characterising data protection. The third path of convergence looks at the evolution of online intermediaries' liability in the field of content and data.

4.1 Constitutional Conflict and Convergence of Values

It is no mystery that the information society has increasingly raised the attention on the protection of freedom of expression, privacy and data protection. In the case of the Union, the threats of new digital technologies implemented by transnational private actors are one of the primary reasons triggering the rise of a new phase of digital constitutionalism. Nevertheless, in this case, what is worth observing does not only concern the risks for these fundamental rights but also the increasing paths of converging values between freedom of expression and data protection.

Even before the advent of online platforms, freedom of expression has met, firstly, privacy as the right to be left alone, and, then, data protection due to the rise of new processing technologies. For instance, the interest to access relevant information for the public interest typically clashes with the right to privacy of the individuals' involved. The notion of 'intellectual privacy' can show the intersection between private sphere and freedom of expression.[73] As underlined by Richards, intellectual privacy is 'a zone of protection that guards our ability to make up our minds freely'.[74] Surveillance affects not only privacy and data protection but also freedom of expression. Users cannot only be concerned about the control of their private spheres but also limit the sharing of their opinion and ideas. This could also happen when digital technologies allowing profiling of users' behaviours is used to manipulate opinions. The conflictual connection between expressions and privacy has become closer through the passing of time. Their interrelation has not basically changed with the rise of the information society. Instead, there has been an amplification of cases where these fundamental rights clash each other.

In the European framework, the scope of the Data Protection Directive confirms this tension between data and content since it did not only introduce a broad notion of personal data but also covered models of processing and disseminating information protected by the right to freedom of expression enshrined in the Charter and the Convention. So that, it is possible to agree that 'from its inception, the entirety of European data protection has been correctly understood to be in inherent tension with such rights'.[75] Even beyond the extensive definitions in the field of data, the Data Protection Directive also provided a specific exemption from data protection obligations

[73] Julie Cohen, 'Intellectual Privacy and Censorship of the Internet' (1998) 8(3) Seton Hall Constitutional Law Journal 693.
[74] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* 95 (Oxford University Press 2015).
[75] David Erdos, 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection' (2015) 52 Common Market Law Review 119, 121.

'solely for journalistic purposes or the purpose of artistic or literary expression […] only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.'[76] It is also possible to observe that, as also indirectly suggested in *Lindqvist*,[77] the Data Protection Directive would already embed a certain balance by allowing data protection to influence the standard of the right to freedom of expression.[78] This system of exemption system would subject the right to freedom of expression to the determination to the logics of the data protection system whose scope broad scope is likely to cover different forms of expressions. There is not a general hierarchy between these two fundamental rights at the European constitutional level. An example of this limit comes from the clauses banning the abuse of rights established both by the Charter and the Convention.[79] Even in *Google Spain*, it is true that the ECJ recognises that the prevalence of the right of the data subjects' fundamental rights over the interest of internet users. At the same time, the ECJ observed that the balance may depend on 'specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life'.[80]

This fight is the result of two different constitutional goals aimed to protect conflicting rights like secrecy and public disclosure. In other words, the meeting of freedom of expression, privacy and data protection is the result of a conflict rather than a convergence between constitutional interest. From this perspective, the relationship between these rights can be defined as adversarial ('freedom of expression v privacy/data protection'). The solution to this natural conflict has traditionally consisted of the balancing between fundamental rights made *ex ante* by lawmakers and *ex post* by courts.[81] At first glance, the conflict between these two rights could be considered a form of convergence since both rights contribute to influencing the scope of protection of each other through the balancing activities. Nevertheless, their clash can also be considered an example of divergence since both systems aim to protect different rights from their constitutional perspective.

Notwithstanding these considerations are still applicable in the algorithmic society, the relationship between freedom of expression, privacy and data protection cannot be seen any longer just as adversary but also as cooperative ('freedom of expression and privacy/data protection'). This cooperation lies in the joint mission underpinning these fundamental rights consisting of protecting democratic values. Freedom of expression, privacy and data protection are pillars of democratic societies. Without expressing opinion and ideas freely, it is not possible to qualify a society as democratic. Likewise, without relying on procedures on the processing of personal data, it would not be possible to safeguard privacy and tackle an imbalance of power

[76] Data Protection Directive (n 1), Art 9. See C131/12 (n 50); Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (2008).
[77] Case C-101/01, Lindqvist (2003) ECR I-12971, 82.
[78] Magdalena Jozwiak, 'Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union. The Vulnerability of Rights in an Online Context' (2016) 23(3) Maastricht Journal of European and Comparative Law 404.
[79] European Convention on Human Rights (1950), Art 17; Charter of Fundamental Rights of the European Union (2012) OJ C326/12. Art 54.
[80] Case C-131/12 (n 50), 81.
[81] Eric Barendt, 'Balancing Freedom of Expression and Privacy' (2009) 1(1) Journal of Media Law 49.

between data controllers and subjects coming from the consolidation of an opaque sphere of data ignorance.

The common mission of these two fundamental rights emerged when examining the rise of a democratic phase of digital constitutionalism. Despite their natural conflictual relationship, both fundamental rights have shown their ability to provide the Union constitutional instruments to answers platforms' powers through the autonomous governance of speech and the degradation of the private sphere. The measures adopted at European level to regulate the process of content moderation and processing of automated decision-making processes are two clear examples of the mission of freedom of expression, privacy and data protection to protect democratic values in the algorithmic society. Their conflictual relationship can also be seen as a cooperative relationship linked by a common democratic goal.

4.2 From Content to Procedure

Another path of legal convergence comes from the legal regime of content approaching the traditional structure on which data protection law is based. European data protection law provides rule governing the procedures for collecting, organising and making available personal data. It determines according to which conditions data should be considered personal, the role and responsibilities of controllers and processors as well as the procedures to follow in the processing of personal data. Failure to comply with this system triggers the liability of data controllers and processors.

The field of content instead is not structured on procedures but on qualifying and tackling illegal content. Put another way, the focus is on the *an* but not on the *quomodo*. The e-Commerce Directive does not introduce safeguards in the processing of content when online intermediaries process them like in the case of content moderation. It just defines the role and responsibilities of online intermediaries to deal with illegal content. Hosting providers are just obliged to remove illegal content based on their awareness without any specific procedure. The e-Commerce Directive leaves Member States free to set further safeguards in this process without however requiring them to ensure a minimum and harmonised standard of protection.[82] The only limit is the ban for Member States to introduce general monitoring obligation applying to online intermediaries.[83] In other words, the data protection law framework does not care whether data are illicit *per se*, but whether their processing is unlawful. On the opposite, in the field of content, the focus is on substantive requirements rather than procedural ones.

The recent steps in the field of the Digital Single Market strategy have highly affected this original legal divergence. The field of content and data looks more similar in terms of structure and obligations. The Copyright Directive and the AVMS Directive highlight this path of convergence. The Copyright Directive introduces several procedural safeguards in online platforms' content moderation of copyright content.[84] For instance, online platforms are required to put in place an effective and expeditious complaint and redress mechanism which users can access to in the event of disputes over the disabling of access to, or the removal of, works or other

[82] E-Commerce Directive (n 1), Recital 46.
[83] Ibid, Art 15.
[84] Copyright Directive (n 65), Art 17.

subject-matter uploaded by them.[85] This obligation leads online platforms to proceduralise their activities like in the field of data. Likewise, the AVMS Directive provides a list of appropriate measures such as the establishment and of mechanisms for users of video-sharing platforms to report or flag to the video-sharing platform provider or age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors. It should also be mentioned that the Union has not abandoned its focus on defining illicit content rather setting managing procedures. The last version of the proposal for a Regulation on terrorist content still tends to define illicit content.[86] According to the proposal, the scope of terrorist is limited according to legal definition including cases of incitement and solicitation.[87] At the same time, the proposal introduces accountability and transparency safeguards in the moderation of terrorist content by hosting providers.[88] Therefore, despite the hybrid solution, this case is another example of how the process of moderation is increasingly going towards procedural obligations like in the field of data.

This first examples of shift from content to procedure is primarily the result of the new phase of digital constitutionalism. Indeed, the threats to freedom of expression coming from private powers online are mostly due to the lack of transparency and accountability in the moderation of content. To solve this imbalance of power, the structural shift in the attention of the Union on 'content procedures' rather than censoring measures to protect the right to freedom of expression has triggered a new path of legal convergence in the algorithmic society.

4.3 Content and Data Liability

The GDPR triggered the third path of legal convergence between content and data, precisely concerning the application of the system of the e-Commerce Directive in the field of data protection. The GDPR underlines that its scope should not affect the application of the rules provided for by the e-Commerce Directive, including the provisions on online intermediaries' liability. However, the provision limiting the scope of the e-Commerce Directive is still in force.

A literal and narrow reading of the e-Commerce Directive would suggest that the liability exemptions only applies to content without concerning the liability of online intermediaries for third-party data protection infringements or the liability of data controller since these matters would be governed by the Data Protection Directive. As a result, even if online platforms can benefit from the exemption of liability established by the e-Commerce Directive, they remain liable for infringements in the field of data. As stated in e-Commerce Directive, '[T]he implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards […] the liability of intermediaries'.[89] At the same time, other passages could be interpreted in the opposite way meaning that data protection rules would prevail over the system of liability established by the e-Commerce Directive. For instance, it states that 'the protection of individuals with regard to the

[85] Ibid, Art 17(9).
[86] 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)).
[87] Ibid, Art 2.
[88] Ibid, Arts 9-11.
[89] E-Commerce Directive (n 1), Recital 14.

processing of personal data is solely governed by [data protection laws], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive'.[90] Consequently, there are two potential interpretations. Firstly, nothing has changed since the GDPR could not affect the scope limitation established by the e-Commerce Directive. Secondly, it is possible to picture a potential clash between the two legislative instruments since the GDPR states that it should not prejudice the application of the e-Commerce Directive, especially concerning online intermediaries' liability, thus, opening the doors towards an extension of online intermediaries exemption of liability in the field of data protection.

In the past, scholars addressed this question supporting the abolition of the 'data protection exceptionalism' according to which online intermediaries could not rely on the exemption of liability for third-party data.[91] The solution would consist of deferring to 'data-protection law for the specification of what processing of personal data is illegal, while giving providers immunity for all illegal processing taking place on their platform (including processing that is illegal because of violations of data protection law)'.[92] This perspective is also confirmed by the potential application of the safe harbour regime only to third-party content. The extension of this regime should not be considered as an exemption of liability the from unlawful processing of personal data performed directly by online intermediaries. Whereas, in relation to online content violating data protection rules, in this case, online intermediaries could rely on the liability regime established by the e-Commerce Directive. The potential applicability of the e-Commerce Directive in the field of data would not put aside the other provision of data protection law. On the opposite, it would just lead to derogating provisions of liability for the distribution and storage of third-party content infringing data protection law which would remain the normative point of reference to assess the lawfulness of users' content.

Nevertheless, in this case, it is worth underlining that an exemption of liability would raise challenges when online intermediaries are also data controller, so they would have an active role in processing third-party content infringing data protection law. Secondly, other limitations to the application of the e-Commerce Directive can also be found from the GDPR itself such as the exclusion of the application of the data protection rules for 'purely personal or household activity'.[93] However, in this last case, it is necessary to mention that Recital 18 excludes these activities from the scope of the GDPR except for the case in which the data controllers or processors provide the means for processing personal data for such personal or household activities.[94] As a result, according to this interpretative provision, even in this case, online intermediaries could be subject to the application of GDPR while they could rely on their exemption of liability in the field of data if users process data within the scope of the aforementioned exception. Thirdly, the lack of any reference to the e-Commerce Directive when the GDPR addresses the liability of data controller and processor does not help to clarify the relationship between the two regimes. Regarding the liability of the data controller, the GDPR

[90] Ibid.
[91] Giovanni Sartor, '"Providers" Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?' (2013) 3(1) International Data Privacy Law 3.
[92] Ibid, 5.
[93] GDPR (n 68), Article 2(2)(c).
[94] Ibid, Recital 18.

provides that a controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. At this point, it would be possible to argue that online intermediaries as passive providers when exercising their functions as data controller or processor should not be considered liable for third-party conducts.[95] It is necessary to observe that, unlike the Data Protection Directive, the GDPR does not provide examples of how a controller might prove the lack of any liability: *force majeure* or error on the part of the data subject.[96] Although the provision could be interpreted in the same meaning that it refers only to events beyond the control of the controller or the processor, however, it is not clear whether even this provision could be used as a defence against third-party illicit behaviours.

These interpretations underline the overlap between the two fields. The extension of the regime of the e-Commerce Directive to third-party content infringing data protection law could also come from a constitutional interpretation based on the balancing between the freedom to conduct business of platforms and users' fundamental rights. It is possible to observe that the extension of the scope of the e-Commerce Directive would increase uniformity in online content moderation.[97] If online intermediaries would be able to rely on the safe harbour against illicit data processing perpetrated by third-party, their process of content moderation could benefit from a general extension also to that online content with the result that this approach would foster the freedom to conduct business of online intermediaries. This is also why Keller underlined that the extension of the e-Commerce rule to the field of data would be a matter of fairness.[98]

Since the e-Commerce Directive allows Member States to impose injunction and filtering systems to online intermediaries to address specific cases, it would be possible to understand how the positive effects of such a system would be mitigated by the risk to proactively monitor also personal data when they are disseminated through their platform to tackle third-party violations. Since the algorithmic society has led online intermediaries to play a more active role processing data and performing content moderation activities, this safe harbour extension could encourage platforms to increase their monitoring activities with potential chilling effects for freedom of expression with troubling effects even on other users' fundamental rights like privacy.[99] Besides, it should also not be neglected that allowing online platforms to benefiting from the exemption of liability even for third-party content infringing personal data could also reduce the guarantees of users vis-à-vis platforms powers. The e-Commerce Directive framework does not provide safeguards in this process, so that users could not complain against platforms' refusal to remove certain data due to the fact that platforms are freely to decide the fate of the information they host, especially when those are not likely illicit like in the case of delisting requests. Instead, the GDPR

[95] Ibid, Art 82(3).
[96] According to Recital 55, '[A]ny damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive'.
[97] Brendan Van Alsenoy, 'Liability under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 9(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 271.
[98] Keller (n 64).
[99] See Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (2011); Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (2012).

recognises data subjects' rights. Even if, as already stressed, this could be an incentive for online intermediaries to extensively monitor their spaces to avoid any failure to comply with obligations, however, it is also a way to require them to take users' request seriously.

As a result, it is worth wondering how *Google Vivi Down and Google Spain* would have been adjudicated if the GDPR was in force at that time. In the lack of judicial interpretation about the two regimes of liability, it is not possible to foresee how the Italian courts and ECJ would have interpreted the two cases. According to this system, as underlined in *La Quadrature du Net*, the ECJ can decide which regime applies by putting aside one of them. One of the primary consequences of this approach is to blur the boundaries between the two regimes, precisely between the notion of 'data controller' and 'active provider' affecting the application of the rules in the field of content and data.

5. The Challenges Ahead in the Field of Content and Data

The relationship between content and data has become self-evident with the rise and consolidation of online platforms. The increasing relevance of the digital environment has led to revolutionary changes in processing information. Different types of data are published and mixed with other information through systems that organise, promote and aggregate content. From a first season of technological and legal divergence at the beginning of this century, the legal regimes of online intermediaries and data have slowly started a dialogue triggered by a trend of technological convergence.

From the first contact in *Promusicae*, such a relationship has become more blurred with the advent of online platforms whose business was based on data-driven models. In *Google Vivi Down* and *Google Spain*, the interpretation of the Italian Courts and ECJ has highlighted the complexities in applying a rigid separation between the two systems. Both layers have started to technologically overlap when focusing on online intermediaries such as search engines and social networks which do not merely perform the activity of data processor or passive provider any longer. The mix of active provider and data controller implies that the rigid distinction in the application of the two regimes (and their parallel track) would not be any longer justified by the passive role of online intermediaries. Put another way, if it is not a surprise that the e-Commerce Directive excluded privacy and data protection matters from its scope of application in 2000, nowadays the same political choice would look different when it is applied to intermediaries like social networks and search engines.

Even if formally the Union has maintained a system based on parallel track even in the framework of the Digital Single Market Strategy, however, some paths of legal convergence increasingly highlight the relationship between freedom of expression and data protection. Despite these historical differences between the two fields in question, freedom of expression and data protection have shown their ability to overcome the aforementioned legal divergence by sharing the common goal to protect democratic values. This trend looks clearer in the phase of digital constitutionalism where the need to protect both fundamental rights led to a positive regulatory reaction by the Union to address the issue for fundamental rights online like in the case of the adoption of the GDPR or the new rules to address platforms' powers in the field of content. Likewise, even the introduction of procedural safeguards is another critical sign of convergence towards the creation of a more transparent and accountable digital environment. The system of

liability in the field of content and data is another example of potential convergence even if, in this case, it is still not clear whether the GDPR would open the doors towards an overlap between the two regimes in terms of responsibilities and liability for third-party content and data.

The two regimes conceived on parallel tracks have shown paths of convergence even before the outbreak of platforms' power. It would not be hazardous to argue that the evolution of artificial intelligence technologies will increasingly lead the two systems to collide where data controllers and hosting providers decide how to exploit the value coming from the interrelation of content and data. The cases of content moderation and automated decision-making processes provide some clues of this evolution. Therefore, they deserve to be further analysed within the framework of European digital constitutionalism to understand the evolution of the protection of fundamental rights and democratic values in the algorithmic society.

Chapter V

Digital Constitutionalism and Freedom of Expression

Summary: 1. Expressions in the Algorithmic Society. – 2. From the Free Marketplace of Ideas… – 3. …To the Algorithmic Marketplace of Ideas. 3.1 The Public Sphere in the Age of Algorithms. 3.2 The Logic of Moderation. 3.3 Private Enforcement of Freedom of Expression. – 4. The First Steps of Digital Constitutionalism. – 5. Horizontal Effect as Filling Regulatory Gaps? – 6. Rethinking Media Pluralism Online. 6.1 Notice System. 6.2 Decision-making. 6.3 Redress. – 7. Expressions as Data.

1. Expressions in the Algorithmic Society

Freedom of expression is one of the cornerstones on which democracy is based.[1] This non-exhaustive statement acquires a specific relevance in the digital environment.[2] In the last twenty years, the Internet has become one of the primary means to exercise rights and freedoms.[3] Thanks to the possibility to access online content ubiquitously, the digital environment plays a crucial role in promoting the sharing of opinion and ideas on a global scale.[4] Nevertheless, this flourishing democratic framework firmly clashes with the troubling evolution of the algorithmic society where online platforms govern the flow of information online.[5] By taking decisions on expressions, they contribute to shaping their right to freedom of expression on a global scale. The relevance of this concern can be understood by observing that more than 2 billion of users are today governed by Facebook's community guidelines,[6] and YouTube decide how to host and distribute billions of hours of video each week.[7]

---

[1] Cass Sunstein, *Democracy and the Problem of Free Speech* (The Free Press 1995).

[2] Jack M. Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79(1) New York University Law Review 1.

[3] Andras Koltay, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere* (Hart 2019); Marco Bassini, *Internet e Libertà di Espressione. Prospettive Costituzionali e Sovranazionali* (Aracne 2019); Marco Betzu, *Regolare Internet. Libertà di informazione e di comunicazione nell'era digitale* (Giappichelli 2012); Anna Papa, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico* (Giappichelli 2009); Vincenzo Zeno-Zencovich, *La libertà di espressione. Media, mercato, potere nella società dell'informazione* (Il Mulino 2004).

[4] Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York University Press 2006).

[5] Niva Elkin-Koren and Maayan Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed.), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020); Sarah T. Roberts, *Behind the Screen. Content Moderation in the Shadows of Social Media* (Yale University Press 2019); Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598; Kyle Langvardt, 'Regulating Online Content Moderation' (2018) 106 The Georgetown Law Journal 1353.

[6] Ben Popper, 'A Quarter of the World's Population now Uses Facebook Every Month' The Verge (3 May 2017) <https://www.theverge.com/2017/5/3/15535216/facebook-q1-first-quarter-2017-earnings>accessed 2 August 2019.

[7] Jack Nicas, 'YouTube Tops 1 Billion Hours of Video a Day, on Pace to Eclipse TV' Wall Street Journal (27 February 2017) <https://www.wsj.com/articles/youtube-tops-1-billion-hours-of-video-a-day-on-pace-to-eclipse-tv-1488220851> accessed 2 August 2019.

This privatised governance of expressions,[8] which is oriented to profit maximisation, would not lead to putting much hope in the role of democratic values online.[9] Nonetheless, it cannot be neglected that political and social engagements have spread in the digital environment.[10] Despite different views, in any case, an oligopoly of private entities organises transnationally online information for profit by using automated technologies.[11] The organisation of social networks' news feed or the results provided by a search engine are only some examples of the role of automated decision-making systems in online content moderation and how online platforms impose their functional sovereignty.[12] Since algorithmic technologies are programmed according to the economic and ethical values of online platforms without any users' involvement, the extent to which users' freedom of expression is protected is subject to private determinations driven by profit maximisation.[13]

The grounding principle of content moderation is to govern users' attention.[14] The frequency of interaction, emotional reactions or comments are just some examples of the information which platforms can extract from users' behaviours. This amount of information is then analysed to influence visibility and engagement which are usually fostered by matching similar content or standpoints according to micro-targeting strategies.[15] The numbers of likes or shares together with the analysis of users' similarities are then used for moderating information online and profiting from advertising revenues.[16] This 'food' for algorithms create filters based on reciprocal interactions which tend to show users content which is related to their algorithmic profile. This is not entirely new but based on the tendency of human to create relationships with people who share their ideas and values, what has been called the 'homophily of networks'.[17] This system also affects political speech by politicians or news media organisations.[18] According to Sajó, 'instead of creating a common space for democratic deliberation, the internet and social media enabled fragmentation and segmentation. Discourse is limited to occur within self-selecting groups and there are tendencies of isolation. Views are more extreme and less responsive to

[8] Andrew Tutt, 'The New Speech' (2014) 41 Hastings Constitutional Law Quarterly 235.
[9] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, 2011).
[10] Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Polity Press 2012).
[11] Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 University of California Davis 1151, 1.
[12] Frank Pasquale, 'From Territorial to Functional Sovereignty: The Case of Amazon' Law & Political Economy Blog (6 December 2017) <https://lpeblog.org/2017/12/06/from-territorial-to- functional-sovereignty-the-case-of-amazon/> accessed 24 July 2019.
[13] Josè Van Dijk and Thomas Poell, 'Understanding Social Media Logic' (2013) 1(1) Media and Communication 2; Tarleton Gillespie, 'The Politics of Platforms' (2010) 12(3) News Media & Society 347.
[14] James G. Webster, 'User Information Regimes: How Social Media Shape Patterns of Consumption' (2010) 104 Northwestern University Law Review 593.
[15] Philipp M. Napoli, *Social Media and the Public Interest: Media Regulation in the Disinformation Age* (Columbia University Press 2019).
[16] Engin Bozdag, 'Bias in Algorithmic Filtering and Personalization' 15(3) Ethics and Information Technology 209.
[17] Miller McPherson, Lynn Smith-Lovin and James M. Cook, 'Birds of a Feather: Homophily in Social Networks' (2001) 27 Annual Review of Sociology 415.
[18] David Tewksbury and Jason Rittenberg, 'Online News Creation and Consumption: Implications for Modern Democracies' in Andrew Chadwick & Philipp N. Howard (eds), *The Handbook of Internet Politics* 186 (Routledge 2008).

external arguments and facts, resulting in polarization around alternative facts'.[19] The activity of content moderation indeed contributes to locking each user within personalised public spheres shaped by opaque business logic. Such a process turns online platforms into a manipulation machine.[20] Put another way, no matter what kind of speech, this is in the filtering hands of social media.

Against such confinement, users cannot still rely on safeguards in the process of content moderation. Platforms do not usually implement transparent procedures explaining to users how their content is organised or provide explanations when removing or blocking expressions. If content moderation plays a crucial role in governing the information flow in the digital environment, it is worth focusing on how to remedy this lack of transparency and accountability to ensure that users are not exposed just to content reflecting business logics rather than pluralism. In a democratic society, citizens should enjoy a degree of autonomy which allow developing their own opinions and participate in decision-making processes. Democracy highly relies on citizens' self-determination, and freedom of expression is not only a fundamental right but also a mean to foster individuals' autonomy as expression of the framework of dignity characterising European constitutionalism.

The informational (and power) asymmetry between users and platforms leads to discussing whether the traditional liberal feature of the right to freedom of expression can ensure democratic values in the algorithm era. Democratic States are open environments for pluralism and values such as liberty, equality, transparency and accountability. On the contrary, the activity of online platforms is based on business interests, opaque procedures and unaccountable decision-making. As examined in Chapter III, the law of the platform competes with the authority exercised by public actors. While online platforms have a responsibility rather than a duty to guarantee the respect of fundamental rights and freedoms, democratic States are required to safeguard these interests to protect the entire democratic system. Such duty also encompasses a positive obligation to protect individuals against acts committed by private persons or entities.[21] Without protecting equality, freedom of expression or assembly, it would not be possible to enjoy a democratic society.

Within this clash between democratic public values and non-democratic business interests, this chapter focuses on the challenges of freedom of expression in the algorithmic society and how European digital constitutionalism can provide remedies to deal with this troubling scenario for democracy and the rule of law. This chapter underlines that the vertical and negative nature of freedom of expression is no longer enough to protect democratic values in the digital environment, since the flow of information is actively organised by business interests, driven by profit-maximisation rather than democracy, transparency or accountability. Therefore, beyond describing the approach of the Union, the normative side of this chapter proposes remedies in the field of content to protect freedom of expression from a constitutional law perspective.

---

[19] European Centre for Press and Media Freedom, 'Promoting Dialogue Between the European Court of Human Rights and the Media Freedom Community. Freedom of Expression and the Role and Case Law of the European Court of Human Rights: Developments and Challenges' (2017) <https://www.ecpmf.eu/archive/files/ecpmf-ecthr_conference_e-book.pdf> accessed 26 April 2020.

[20] Siva Vaihyanathan, *Anti-Social Media* (Oxford University Press 2018).

[21] UN Human Rights Committee (HRC), 'General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant', 26 May 2004 <https://www.refworld.org/docid/478b26ae2.html> accessed 7 October 2019.

In order to achieve this aim, the first part of this chapter analyses the shift from a liberal economic narrative based on the metaphor of the free marketplace of ideas to the rise of online platforms power in moderating online content. Precisely, it focuses on the logic of content moderation, the rise of the algorithmic public sphere and the challenges to the protection of the right to freedom of expression raised by the private enforcement of fundamental rights. This part shows how the development of the information society has challenged the liberal paradigm of free speech requiring a complementary shift from a negative to a positive dimension. The second part focuses on the current *status quo*, underlining the lack of safeguards on which the users can rely vis-à-vis online platforms and focusing on the horizontal effect doctrine as a potential way to fill the regulatory gap in the field of content moderation. The fourth part supports a normative approach to media pluralism online which does not focus on platforms' liability but on users' safeguards fostering democratic values in the digital environment.

2. From the Free Marketplace of Ideas…

The right to freedom of expression in modern and contemporary history has liberal roots. Like other civil and political liberties arisen at the end of the XIX century,[22] the right to free speech is based on the idea that liberties and freedoms can be ensured by limiting interferences coming from public actors.[23] The possibility to express opinion and ideas freely is the grounding condition to develop personal identity and ensures the right to self-determination in a democratic society.

It is not by chance that that one of the most suggestive legal metaphors in this field is that of the 'free market place of ideas',[24] as coined for the first time by Justice Douglas in *United States v Rumely*.[25] This liberalist belief can be contextualised in the classical theory of market balance

[22] The Declaration of the Rights of Man and of the Citizen (1789).

[23] Eric Barendt, *Freedom of Speech* (Oxford University Press 2017); Corrado Caruso, *La libertà di espressione in azione. Contributo a una teoria costituzionale del discorso pubblico* (Bononia University Press 2013); Alessandro Pace and Michela Manetti, 'Articolo 21', in Giuseppe Branca (ed.), Commentario della Costituzione (Zanichelli 2006); Michela Manetti, 'La libertà di manifestazione del pensiero' in Roberto Nania and Paolo Ridola (eds), *I diritti costituzionali,* vol. II, 549 (Giappichelli 2001); Massimo Luciani, 'La libertà di informazione nella giurisprudenza costituzionale italiana' (1989) (4) Politica del diritto 605; Paolo Barile, *Liberta di manifestazione del pensiero* (Giuffrè 1975); Vezio Crisafulli, 'Problematica della "libertà di informazione"' (1964) 29(2) Il Politico 285; Carlo Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano* (Giuffrè 1958); Sergio Fois, *Principi costituzionali e libera manifestazione del pensiero* (Giuffrè 1957).

[24] Daniel E. Ho and Frederik Schauer, 'Testing the Marketplace of Ideas' (2015) 90 New York University Law Review 1161; Eugene Volokh, 'In Defense of the Market Place of Ideas / Search for Truth as a Theory of Free Speech Protection' (2011) 97(3) Virginia Law Review 591; Joseph Blocher, 'Institutions in the Marketplace of Ideas' (2008) 57(4) Duke Law Journal 820; Paul H. Brietzke, 'How and Why the Marketplace of Ideas Fails' (1997) 31(3) Valparaiso University Law Review 951; Alvin I. Goldman and James C. Cox, *Speech, Truth, and the Free Market for Ideas* (Cambridge University Press 1996).

[25] United States v Rumely 345 U.S. 41 (1953). 'Of necessity I come then to the constitutional questions. Respondent represents a segment of the American press. Some may like what his group publishes; others may disapprove. These tracts may be the essence of wisdom to some; to others their point of view and philosophy may be anathema. To some ears their words may be harsh and repulsive; to others they may carry the hope of the future. We have here a publisher who through books and pamphlets seeks to reach the minds and hearts of the American people. He is different in some respects from other publishers. But the differences are minor. Like the publishers of newspapers, magazines, or books, this publisher bids for the minds of men in the market place of ideas'.

applied to the field of ideas.[26] Since individuals act rationally, they can choose the best products and services in a free market. As in a competitive market where the best products or services prevail, the same mechanism would apply to the best information resulting from market balance.

However, the liberal grounds of freedom of expression are more-in-depth and older. In the seventeenth century, Milton, opposing to the English Parliament's Press Ordinance, which had introduced a system of censorship to punish the promoters of ideas considered illegal, argued that freedom of expression should not be limited to allow the truth to prevail thanks to the free exchange of opinion.[27] Milton compares the truth to a streaming fountain whose water constitutes the flow of information saving men from prejudice. According to this perspective, it is necessary to avoid any interference with the flow of information to lead men to the highest level of knowledge. Two centuries later, Mill shared a liberal approach to freedom of expression.[28] Even falsehood could contribute to reaching the truth.[29] Otherwise, censoring falsehood would make meaningless the comparison between ideas and opinions with the risk of dogmatising the current truth.[30] Both Milton and Mill agreed that the right to freedom of expression is effective when it is free from censorship and powers' interferences.

The scope of these liberal ideas opposing public actors' interferences also emerged in the US legal framework.[31] The Justice Holmes' dissenting opinion in *Abrams v United States* can still be considered the constitutional essence of freedom of expression in the United States as enshrined in the First Amendment.[32] The case concerned the distribution of leaflets calling for ammunition factories to strike to express a clear message of resistance against the US military intervention in Russia. According to Justice Holmes, although men try to support their positions by criticising opposing ideas, they must not be persuaded that their opinions are certain. Only the free exchange

---

[26] Ronald Coase, 'Markets for Goods and Market for Ideas' (1974) 64(2) American Economic Review 1974.

[27] John Milton, *Aeropagitica* (1644). According to Milton: 'So Truth be in the field, we do injuriously, by licensing and prohibiting, to misdoubt her strength. Let her and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter?'.

[28] John S. Mill, *On Liberty* (1859).

[29] Ibid, 'First, if any opinion is compelled to silence, that opinion may, for aught we can certainly know, be true. To deny this is to assume our own infallibility'.

[30] Ibid, 'Thirdly, even if the received opinion be not only true, but the whole truth; unless it is suffered to be, and actually is, vigorously and earnestly contested, it will, by most of those who receive it, be held in the manner of a prejudice, with little comprehension or feeling of its rational grounds. And not only this, but, fourthly, the meaning of the doctrine itself will be in danger of being lost, or enfeebled, and deprived of its vital effect on the character and conduct: the dogma becoming a mere formal profession, inefficacious for good, but cumbering the ground, and preventing the growth of any real and heartfelt conviction, from reason or personal experience'.

[31] Giovanni Bognetti, *Lo spirito del costituzionalismo americano: breve profilo del diritto costituzionale degli Stati Uniti* (Giappichelli 2000); Giovanni Bognetti, *La libertà d'espressione nella giurisprudenza americana. Contributo allo studio dei processi dell'interpretazione giuridica* (Istituto Editoriale Cisalpino 1958).

[32] Abrams v United States (1919) 250 U.S. 616, 'Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition [...] But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas. […] The best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out'.

of ideas can confirm the accuracy of each position.[33] Freedom of speech is functional to ensure that individuals are autonomous and, therefore, responsible moral agents participating in a political society.[34] According to Meiklejohn, the constitutional protection of free speech aims to foster citizens' awareness about public matters.[35]

This liberal approach has also been expressed, more recently, in the framework of the digital environment, at least in two landmark decisions of the US Supreme Court. In 1997, in *Reno v ACLU*,[36] the Supreme Court ruled that the provisions of the CDA concerning the criminalisation of obscene or indecent materials to any person under 18 was unconstitutional.[37] As observed by the Supreme Court, unlike traditional media outlets, 'the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material'.[31] According to Justice Stevens, the Internet plays the role of a 'new marketplace of ideas' observing that 'the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship'.[38] Besides, '[t]he record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship'.[39] This can be considered the first step towards the end of the public forum doctrine.[40]

In the aftermath of the Internet, the optimist interpretation of the US Supreme Court was also reflected by the theories of those scholars who considered the Internet as a new place outside the interference of any public actor.[41] However, this approach has been generally questioned by whom had already underlined an increasing discretion of new actors in the cyberspace,[42] deriving also from the private enforcement of public policies online.[43] In the aftermath of the Internet, this decision represented the ground to build a democratic culture where everyone can share opinion and ideas with other communities, access more information and express their personal identity.

Despite the passing of years and opposing positions, this liberal approach has been reiterated more recently in *Packingham v North Carolina*.[44] The case involved a statute banning registered sex offenders from accessing social networking services to avoid any contact with minors. The

---

[33] See Sheldon Novick, *Honorable Justice* (Laurel 1990).
[34] Ronald Dworkin, *Freedom's Law: The Moral Reading of the American Constitution* (Oxford University Press 1999).
[35] Alexander Meiklejohn, *Free Speech and its Relation to Self-Government* (Lawbook Exchange 2011).
[36] Reno v American Civil Liberties Union 521 U.S. 844 (1997).
[37] Communication Decency Act (1996).
[38] 521 U.S. 844 (n 36).
[39] Ibid, 885.
[40] Dawn C. Nunziato, 'The Death of The Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115.
[41] John P Barlow, 'A Declaration of Independence of the Cyberspace' (Electronic Frontier Foundation, 1996) <www.eff.org/cyberspace-independence> accessed 2 July 2019; David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1371.
[42] Lawrence Lessig, *Code: And Other Laws of Cyberspace. Version 2.0* (Basic Books 2006).
[43] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006); Joel R Reidenberg, 'States and Internet Enforcement' (2004) 1 University of Ottawa Law & Technology Journal 213.
[44] Packingham v North Carolina (2017) 582 U.S. ___.

US Supreme Court placed the Internet and social media on the same layer of public places where First Amendment enjoy a broad scope of protection. In the words of Justice Kennedy: 'It is cyberspace – the "vast democratic forums of the Internet" in general, and social media in particular'.[45] The metaphor of the (digital) free marketplace of ideas is still firm in the jurisprudence of the US Supreme Court. Social media are indeed considered as an enabler of democracy rather than a threat for public discourse. This explains why social media enjoy a safe constitutional area of protection under the First Amendment, which, in the last twenty years, has constituted a fundamental ban on any attempt to regulate speech online,[46] thus, showing the role of First Amendment in US constitutionalism,[47] as the 'the paramount right within the American constellation of constitutional rights'.[48]

Nevertheless, it would be enough just to cross the Atlantic to understand how this general trust for a vertical paradigm of free speech is not shared worldwide by other democracies, especially when the right to freedom of expression is framed in the digital environment. While, in the US, the Internet and social media still benefit from the frame coming from the traditional liberal metaphor of the free marketplace of ideas as a safeguard for democracy, in Europe, freedom of expression online does not enjoy the same degree of protection.[49] In the European framework, the right to freedom of expression is subject to a multilevel balancing,[50] precisely with other rights enshrined in the Charter,[51] Convention,[52] and national constitutions.[53] Unlike the US Supreme Court, the Strasbourg Court has shown a more restrictive approach to the protection of the right to freedom of expression in the digital environment, perceived more like a risk rather than an opportunity for the flourishing of democratic values.[54]

---

[45] Ibid.

[46] See, e.g., Ashcroft v Free Speech Coalition (2002) 535 U.S. 234; Aschroft v American Civil Liberties Union (2002) 535 US 564.

[47] Lee C. Bollinger and Geoffrey R. Stone (eds), *The Free Speech Century* (Oxford University Press 2019); Floyd Abrams, *The Soul of the First Amendment* (Yale University Press 2017); Frederik Schaurer, 'The Exceptional First Amendment', in Michael Ignatieff (ed.), *American Exceptionalism and Human Rights* 29 (Princeton University Press 2005); Alexander Meiklejohn, 'The First Amendment is an Absolute' (1961) The Supreme Court Review 245.

[48] Michel Rosenfeld and Andras Sajo, 'Spreading Liberal Constitutionalism: An Inquiry into the Fate of Free Speech Rights in New Democracies' in Sujit Choudhry (ed.), *The Migration of Constitutional Ideas* 152 (Cambridge University Press 2007).

[49] Oreste Pollicino and Marco Bassini, 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis', in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* 508 (Edward Elgar 2014).

[50] Ingolf Pernice, 'The Treaty of Lisbon: Multilevel Constitutionalism in Action' (2009) 15(3) Columbia Journal of European Law 349.

[51] Charter of Fundamental Rights of the European Union (2012) OJ C326/12. Art. 11, 52. Filippo Donati, 'Art. 11 – Libertà di espressione e di informazione' in Raffaele Bifulco, Marta Cartabia and Alfonso Celotto (eds*), L'Europa dei diritti – Commento alla Carta dei diritti fondamentali dell'Unione europea* 100 (Il Mulino 2001); Roberto Mastorianni and Girolamo Strozzi, 'Commento all'art. 11' in Roberto Mastroianni and others (eds), *Carta dei diritti fondamentali dell'Unione Europea* 217 (Giuffrè 2017).

[52] European Convention on Human Rights (1950). Art 10. Paolo Caretti, 'Art. 10 – Liberta di espressione' in Sergio Bartole, Benedetto Conforti and Guido Raimondi (eds)*, Commentario alla convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali* 337 (Cedam 2001).

[53] Marco Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione* (Giappichelli 2014).

[54] Oreste Pollicino, 'Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the World of Bits: The Case of Freedom of Speech' (2019) 25(2) European Law Journal 155.

Such a cautious approach in Europe does not only aim to balance different constitutional interests but also avoid that granting absolute protection to one right could lead to the destruction of other fundamental interests undermining de facto their constitutional relevance.[55] This is an expression of the different understanding of the role of dignity on the western side of the Atlantic as mentioned in Chapter I. In Europe, freedom of expression is not indeed a liberal value whose protection needs to be safeguarded at any cost to protect democracy. Allowing such an approach would also entail that speech could be used as a constitutional excuse to hinder democratic values. From a European constitutional perspective, freedom of expression is instead a fundamental right whose protection needs to take into account the other constitutional interests at stake. Unlike the frame of liberty in the US constitutional framework, freedom of expression in Europe does not enjoy absolute protection, but it is subject to the logic of balancing intimately connected to human dignity.[56] As Bognetti underlined, '[i]n European systems there is more reluctance to read freedom of speech in ways that would sacrifice other constitutional values, such as the security of the state or important interests of the person, such as reputation, honour or privacy. At times the necessity of preserving the values of liberal democracy has been felt so intensely as to lead to the prohibition of political parties and to deny legitimacy to speech that has been seen to undermine these values'.[57]

This non-exhaustive framework provides clues to understand why the Union has not adopted an omissive approach to the challenges to freedom of expression raised by the algorithmic society, thus, paving the way towards a new approach, precisely focusing on regulating the process of content moderation. Despite the difference in the protection of the right to freedom of expression in the EU and the US, this fundamental right is still the pre-requisite for a democratic society. However, in the digital environment, the protection of this fundamental right is no longer a matter of quantity but quality because the crucial role of online platforms in determining the standard of protection of freedom of expression and other fundamental rights on a global scale. The case of disinformation is a paradigmatic example of the challenges to the right to freedom of expression in the information society.[58] In other words, the primary challenge for democracies is no longer protecting freedom of expression extensively by granting access to new digital channels and

[55] Charter (n 51), Art 54; Convention (n 52), Art 17.

[56] Mattias Kumm and Alec D. Walen, 'Human Dignity and Proportionality: Deontic Pluralism in Balancing' Grant Huscroft and others (eds), *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (Cambridge University Press 2014).

[57] Giovanni Bognetti, 'The Concept of Human Dignity in U.S. and European Constitutionalism' in Georg Nolte (ed.), *European and US Constitutionalism* 77 (Cambridge University Press 2005).

[58] Giovanni Pitruzella and Oreste Pollicino, Disinformation and Hate Speech: An European Constitutional Perspective (Bocconi University Press 2020); Oreste Pollicino, Giovanni De Gregorio and Laura Somaini, 'Europe at the Crossroad: The Regulatory Conundrum to Face the Raise and Amplification of False Contents Online' (2020) 18 The Global Community Yearbook of International Law and Jurisprudence 2019 319; Oreste Pollicino and Elettra Bietti, 'Truth and Deception across the Atlantic. A Roadmap on Disinformation in the US and Europe' (2019) 11(1) Italian Journal of Public Law 43; Marco Bassini and Giulio E. Vigevani, 'Primi appunti su fake news e dintorni' (2017) (1) Rivista di diritto dei media 11; Oreste Pollicino, 'Fake News, Internet and Metaphors' (2017) (1) Rivista di diritto dei media 23; Cesare Pinelli, '"Postverita", verità e libertà di manifestazione del pensiero' (2017) (1) Rivista di diritto dei media 41; Marco Cuniberti, 'Il contrasto alla disinformazione in rete' (2017) (1) Rivista di diritto dei media 26; Francesco Pizzetti, 'Fake news e allarme sociale: responsabilità, non censura' (2017) (1) Rivista di diritto dei media 48.

avoiding public actors' interferences but ensuring that users can effectively enjoy their rights and freedoms in a democratic digital environment.

3. …To the Algorithmic Marketplace of Ideas

At the World Summit on the Information Society in 2004, Lessig underlined the significant potentialities afforded by the digital environment: '[f]or the first time in a millennium, we have a technology to equalize the opportunity that people have to access and participate in the construction of knowledge and culture, regardless of their geographic placing'.[59] Likewise, Shapiro stated: 'Hierarchies are coming undone. Gatekeepers are being bypassed. Power is devolving down to "end users" [...] No one is in control except you'.[60] These are positive news for the free marketplace of ideas doctrine. Unlike in the atomic world, information sources have spread online. The new online communication channels have enabled users to potentially reach a global audience without relying any longer on the traditional channels of communications where editorial decisions are in the hand of publishers like newspapers and televisions.[61] Put another way, the Internet as a new channel of communication could overcome the problem of concentration of power in traditional media warned by Habermas.[62]

Although it is true that the possibility for users to express opinion and ideas without traditional filters cannot be contested, nonetheless, the lack of control over information online has revealed to be just a libertarian dream. It is true that users can still run their blogs and website to share their ideas or opinions. However, it would be naïve to believe that this is how most of information flows online. To exercise the right to freedom of expression online is almost necessary to rely on online platforms, primarily social media. Users enter into network environments whose governance is in the hands of very few private actors. These entities aim to maximise their profit, and expressions – to say nothing of data – are the perfect means to achieve this purpose. By processing content, platforms can extract information, collecting data and, even mapping emotions to provide the most granular advertising services on the market and finding new ways to attract customers.[63] It would be enough to observe the business models of Facebook and Google based on more than 80% on advertising revenues coming from advertising services.[64] Just these two platforms absorb 75% of the $73 billion digital advertising market in the US.[65] In other words, users are subject to the private governance of the space where information flows based on platforms' business logic.

---

[59] Lawrence Lessig, 'An Information Society: Free or Feudal' (2004) World Summit on the Information Society (WSIS), <http://www.itu.int/wsis/docs/pc2/visionaries/lessig.pdf> accessed 4 August 2019.
[60] Andrew L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World we Know* 11, 30 (Public Affairs 1999).
[61] Jack M. Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296.
[62] Marianne Franklin, *Digital Dilemmas: Power, Resistance, and the Internet* (Oxford University Press 2013).
[63] Vindu Goel, 'Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry' The New York Times (29 June 2014) <https://www.nytimes.com/2014/06/30/technology /facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html> accessed 24 January 2020.
[64] Mathew Ingram, 'How Google and Facebook Have Taken Over the Digital Ad Industry' Fortune (4 January 2017) <https://fortune.com/2017/01/04/google-facebook-ad-industry/> accessed 2 February 2020.
[65] Shannon Bond, 'Google and Facebook Build Digital Duopoly' Financial Times (14 March 2017) <ft.com/content/30c81d12-08c8-11e7-97d1- 5e720a26771b> accessed 27 January 2020.

The moderation of expressions for profit reflects the logic of digital capitalism,[66] or better information capitalism which leads platform to express surveillance and governance as expressions of powers.[67] At first glance, there would be not so many differences with traditional media outlets governing and filtering information as Habermas criticised. Nonetheless, in the digital environment, the source of platform power comes primarily from new automated processing technologies processing vast amounts of data and information that platforms can accumulate, revealing users so intimate information which is enormous valuable for commercial interests, governments' public tasks and political campaigns. If these considerations are mixed with the choice to exempt online intermediaries from liability for hosting third-party content, it should not surprise how much it could be good for platforms to profit without responsibility. In other words, platforms profit from governing speech without being accountable.

The private governance of content frames users' freedom of expression in a mercantilist environment outside any democratic value. The role of algorithms in organising content has also positive effects to help users to interact and access the information they want in a framework of scarcity of time and attention.[68] Information has spread online with the result of what is now scarce is not the mean but the attention of the listeners.[69] This change has led to the emergence of the attention economy.[70] The price to pay for such intermediation consists of accepting the private values translated by algorithmic determinations. If social media program their algorithmic to achieve business purposes through content moderation, it should not come as a surprise whether content moderation does not reflect necessarily democratic values like diversity or truthfulness. The primary goal is just increasing the probability of an interaction between users and the time and quantity of content they share on social media' spaces. Even more importantly, such discretion in the organisation of expressions also affects the standard of freedom of expression online and the principle of the rule of law. As examined in Chapter III, when removing content, platforms enforcing their internal rules after balancing the interests at stake based on their internal guidelines.

These considerations would explain why considering public actors as the only threat to freedom of expression online could seem anachronistic today. A further challenge raised by the information society concerns how to address the discretion of private actors freely influencing the limits of freedom of expression on a global scale without any public guarantee. The metaphor of the marketplace of ideas is critical now more than ever to represent the current situation, but with a small makeup. The difference consists of the change of the expression 'free' with 'algorithmic' that moves the perspective from democratic and collective values to business and individualist purposes. Ideas do not reach a market balance through the invisible hand, but they are driven by oligopolist logics where decisions are centralised. In the algorithmic marketplace of ideas, speech is still central but not from the perspective of users' freedoms but the platforms' profits. Within

[66] Zeynep Tufekci, 'Algorithmic Harms Beyond Facebook And Google: Emergent Challenges of Computational Agency' (2015) 13 Colorado Technology Law Journal 303.
[67] Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[68] Natali Helberger, 'On the Democratic Role of News Recommenders' (2019) 7(8) Digital Journalism 993.
[69] Herbert A. Simon, 'Designing Organizations for an Information-Rich World' in Martin Greenberger (ed.), *Computers, Communications, and the Public Interest* 37 (Johns Hopkins Press 1971).
[70] Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside our Heads* (Knopf 2016).

this framework, the following subsections focus on the characteristics of the algorithmic public sphere, the logic of moderation and the private enforcement of freedom of expression online.

3.1 The Public Sphere in the Age of Algorithms

'Imagine a future in which your interface agent can read every newswire and newspaper and catch every TV and radio broadcast on the planet, and then construct a personalised summary. This kind of newspaper is printed in an edition of one'. These were the words of Negroponte in 1995 in the aftermath of the Internet.[71] The situation of centralisation and personalisation of expression which users are experiencing in the information society was already there in these sentences.

In the algorithmic society, online platforms mediate the ability of users to share their opinion and ideas online. Using Google or Facebook would constitute almost a mandatory step for entering the public debate and build social interactions online.[72] Already in 1962, Habermas observed that 'the process in which societal power is transformed into political power is as much in need of criticism and control as the legitimate exercise of political domination over society'.[73] The lack of control in the shift from social to political is what already happened in the field of traditional media outlets. Once again, Habermas has already underlined the debasement of the public sphere consisting of the high societal barriers to access channels of communication (e.g. print media) and the intertwined relationship with politics.[74] In this bottleneck, a bunch of national mass media institutions governed public discourse.

These considerations would not sound new when we focus on the digital environment. Like any other libertarian dream, the idea of an alternative world overcoming traditional forms of control failed. As Fraser explained, it is not possible to think a public sphere free from manipulation in a capitalist economy where different forces tend to influence the formation of the public opinion and societal beliefs.[75] Benkler already underlined how the digital environment projects users in a 'networked public sphere'.[76] The difference is the mediating subject which has changed from a bunch of traditional media outlets to an oligopoly of computer networks' providers. While, at first glance, the digital environment could be a solution to overcome centralised powers in the media sector, realising the Habermas' dream of a bourgeois public sphere, a closer look shows how similar dynamics of centralisation and control over information has been reproduced in the digital environment creating a quasi-public sphere.[77] Platforms' ability to massively organise or amplify certain voices (and decide how to do that) leads to thinking about the future of the public sphere online.

---

[71] Nicholas Negroponte, *Being Digital* 153 (Alfred A Knopf 1995).
[72] Taina Bucher, 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook' (2012) 14(7) New Media & Society 1164.
[73] Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* 210 (MIT Press 1991).
[74] Jürgen Habermas, *Between Facts and Norms* (MIT Press 1998).
[75] Nancy Fraser, 'Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy' (1990) 25/26 Social Text 56.
[76] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006).
[77] Jillian C. York, 'Policing Content in the Quasi-Public Sphere' Open Net Initiative' Bulletin (September 2010) <https://opennet.net/policing-content-quasi-public-sphere> accessed 2 February 2020.

At the same time, the digital environment has provided new opportunities to express ideas and opinions. Although the rise of information pluralism should generally be welcomed for the development and maintenance of a democratic environment, the characteristics of the information flow online and its moderation raise serious concerns in terms of pluralism from a perspective of 'quantity' and 'quality'.

From a quantitative perspective, in the last twenty years, a high degree of concentration of the online platforms' market has characterised the digital environment. As foreseen by Zittrain,[78] the characteristics of the information society have led to the creation of monopolies,[79] linked to the platformisation of the Internet,[80] which Srnicek would call the era of 'platform capitalism'.[81] This market concentration empowers a limited number of platforms to set the conditions on which a vast amount of content and data flow online. The effect of this process is to create barriers for entering into the market of information and increase the dependency of traditional media outlets from the new opportunities of visibility offered by social media. Notwithstanding, at first glance, the digital environment has empowered users to access new channels to share ideas and access sources of information, however, the aforementioned digital convergence dangerously affects media pluralism from a quantitative perspective.

From a qualitative standpoint, pluralism is based on different manifestations of thinking and promotes heterogeneous ideas. Instead, in the digital environment, the use of artificial intelligence for online content moderation mitigates this positive effect. As the European High-Level Expert Group on Media diversity underlined the negative impact on democracy since 'increasing filtering mechanisms make it more likely for people to only get news on subjects they are interested in, and with the perspective, they identify with' while '[this reality] will also tend to create more insulated communities as isolated subsets within the overall public sphere'.[82] Democracy indeed needs a public sphere where the meeting of ideas and opinions can be a 'societal glue'.[83] Otherwise, individuals are likely to be attracted by extreme and dogmatic poles, forgetting the alternative ideas which are the basis for consensus in a democratic society. The Habermasian idea of the public sphere is hard to realise in the digital environment where ideas are formulated, negotiated and distributed by machines. In other words, the public sphere in the age of algorithms is not under the control and guidance of public opinion but instead is governed by opaque business purposes.

In a footnote within a larger article of 2006, Habermas underlined that 'computer-mediated communication in the web can claim unequivocal *democratic* merits only for a special context: It can undermine the censorship of authoritarian regimes that try to control and repress public opinion. In the context of liberal regimes, the rise of millions of fragmented chat rooms across the world tends instead to lead to the fragmentation of large but politically focused mass audiences

[78] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press 2008).
[79] Robin Mansell and Michele Javary, 'Emerging Internet Oligopolies: A Political Economy Analysis' in Arthur S. Miller and Warren J. Samuels (eds), *An Institutionalist Approach to Public Utilities Regulation* (Michigan State University Press 2002).
[80] Anne Helmond, 'The Platformization of the Web: Making Web Data Platform Ready' (2015) 1(2) Social Media + Society 1.
[81] Nick Srnicek, *Platform Capitalism* (Polity Press 2016).
[82] High-Level Group on Media Freedom and Pluralism, 'A free and pluralistic media to sustain European democracy' (2013), 27 <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/HLG%20Final%20Report.pdf> accessed 28 January 2020.
[83] Cass R. Sunstein, *Republic.com* 9 (Princeton University Press 2002).

into a huge number of isolated issue publics'.[84] Despite the critics and delusion relating to this non-exhaustive comment,[85] these sentences underline the double face of the online public sphere: a great opportunity for democracy as a liberation technology, but also as a risk for the fragmentation of the public sphere driven by business purposes. According to Habermas, a solid democracy is highly dependent on the public opinion. The shift from 'public' to 'artificial' opinion due to the lack of ability of individuals to act as rational agents is one of the reasons why democracy could be threatened in the information society. Such a liberal root of the public sphere, naturally and deeply connected with that of freedom of expression, is not just put under pressure. It is basically frustrated. It is worth wondering how individuals can be rational users in the algorithmic public sphere if they are subject to a top-down power exercised by online platforms driving the public sphere through artificial intelligence systems whose decision-making processes cannot be always explained. In other words, the same failure of freedom of expression as a negative right to protect democratic values extends even to the liberal vision of the digital public sphere.

A liberal approach to the public sphere based on users' autonomy and rationality seems not to be enough to ensure democratic values any longer. The shift from the 'free' to the 'algorithmic' marketplace of ideas has shown the fallacies of the traditional instruments of pluralism when implemented in the digital environment. Accessing more information could not mean accessing better information. The organisation of content aims to engage users based on their data and preferences, leading to the polarisation of the debate due to the creation of 'filter bubbles' or 'information cocoons',[86] which Sunstein defines as 'communication universes in which we hear only what we choose and only what comforts us and pleases us'.[87] The personalisation of online content leads to the creation of echo chambers where each user is isolated and marginalised from opposing positions as resulting from a mere algorithmic calculation. In other words, users are encouraged to interact only with information inside the area of their preferences.[88]

---

[84] Jurgen Habermas, 'Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research' (2006) 16(4) Communication Theory 411, 423.

[85] Howard Rheingold, 'Habermas Blows Off Question about the Internet and the Public Sphere', SmartMobs (5 November 2007) <http://www.smartmobs.com/2007/11/05/habermas-blows-off-question-about-the-internet-and-the-public-sphere/> accessed 8 February 2020. See, Stuart Geiger, 'Does Habermas Understand the Internet? The Algorithmic Construction of the Blogo/Public Sphere' (2009) 10(1) Gnovis: A Journal of Communication, Culture, And Technology <http://www.gnovisjournal.org/2009/12/22/does-habermas-understand-internet-algorithmic-construction-blogopublic-sphere/> accessed 8 February 2020.

[86] Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (Viking 2011); Cass R. Sunstein, *Republic.com 2.0* (Princeton University Press 2007).

[87] Cass R. Sunstein, *Infotopia: How Many Minds Produce Knowledge* 9 (Oxford University Press 2006).

[88] Empirical evidences of filter bubbles are scarce. See, e.g., see Judith Moeller and Natali Helberger, 'Beyond the Filter Bubble: Concepts, Myths, Evidence and Issues for Future Debates. A Report Drafted for the Dutch Media Regulator' (2018) <https://dare.uva.nl/search?identifier=478edb9e-8296-4a84-9631-c7360d593610> accessed 9 May 2020; Richard Fletcher and Rasmus K. Nielsen, 'Are News Audiences Increasingly Fragmented? A Cross-National Comparative Analysis of Cross-Platform News Audience Fragmentation and Duplication' (2017) 67(4) Journal of Communication 476; Ivan Dylko and others, 'The Dark Side of Technology: An Experimental Investigation of the Influence of Customizability Technology on Online Political Selective Exposure' (2017) 73 Computers in Human Behavior 181; Walter Quattrociocchi and others, 'Echo chambers on Facebook' (2016) The Harvard John M. Olin Discussion Paper Series <http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein _877.pdf> accessed 14 March 2020.

There are already studies showing the role of algorithmic bias in reflecting and amplifying existing human believes.[89] This should not surprise since this process is nothing else of the logic of moderation above mentioned. Personalisation, more than removal or organisation, indeed allows platforms to maximise attention online,[90] thus, meeting the interests of companies interested in advertising their products and services online. Social media exploits the characteristics of human communication based on the tendency to avoid dissensus.[91] Since advertising revenues are highly dependent on attracting scarce attention, discovering new ways to manipulate users' behaviours is the mission of what Zuboff would define as 'surveillance capitalism'.[92]

Automation is implemented not only to remove but also organise and recommend content, thus, influencing users' interactions. It would be enough to think about how the search results of Google or the Facebook newsfeed are not the same for each individual,[93] but they create what, at the beginning of this century, has been already defined as distinguished public spheres.[94] Micro-targeting aims to limit the audience to certain content to increase the likelihood of capturing attention. While, like price discrimination, this is not an issue in the market field, it is instead when this practice is applied to the democratic debate that it shows how believing in a uniform public sphere in the information society could not be possible. Micro-targeting strategies intentionally focus just on certain groups giving the possibility to reach only those who are potentially interested in that content, no matter if the information is of commercial or political nature.[95]

Although traditional media outlets could be accused of filtering relevant news or even manipulating information, they just provide unique platforms to discuss. On the opposite, online platforms create different places driven by business purposes for each user. Algorithms can indeed decide what deserves to be on top and what instead it is better to hide. They choose who is a best friend rather than recommending that journal article or blog post to read. By processing a vast amount of information and data, artificial intelligence systems can select the relevant item to put in front of the user's eyes. The problem is that information that is relevant for the public debate is not defined by the exchange of views and opinions but machines. These systems are far from being perfect, leading to potential discriminatory bias or to exposure to objectionable content.[96]

---

[89] Safiya U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018).
[90] Bozdag (n 16).
[91] Leon Festinger, *A Theory of Cognitive Dissonance* (Stanford University Press 1957).
[92] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).
[93] Micheal A. DeVito, 'From Editors to Algorithms' (2017) 5(6) Digital Journalism 753.
[94] There is not a unitary notion of public sphere. See, e.g., Todd Gitlan, 'Public Sphere or Public Sphericules?' in Tamar Liebes and James Curran (eds), *Media, Ritual and Identity* 168 (Routledge 2002); Micheal Warner, *Publics and Counterpublics* (MIT University Press 2002); Catherine R. Squires, 'Rethinking the Black Public Sphere: An Alternative Vocabulary for Multiple Public Spheres' (2002) 12(4) Communication Theory 446.
[95] Frederik J. Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82.
[96] Muhammad Ali and others, 'Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes' in *Proceedings of the ACM on Human-Computer Interaction* (ACM 2019); Reuben Binns and others, 'Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation' in Giovanni L. Ciampaglia, Afra Mashhadi and Taha Yasseri. *Social Informatics* 405 (Springer 2017).

Therefore, there are intertwined public spheres whose sum then makes the single (and invisible) public sphere. This is also why, according to Schudson, the public sphere was never entirely based on agents' rational independency.[97] It has been always shaped by a form of intimate tribality governing the transmission of knowledge and ideas across society. What makes the public sphere is the sense of community or namely the function of communication towards building a global village,[98] where people consume information to underline their connection and define their place in the world.

Within this framework, users have no information about what happens behind the screen. Between self-selected and pre-selected personalisation, also known as explicit or implicit personalisation,[99] the latter mostly prevail over the former.[100] In the first case, users have more discretion in defining the criteria according to which online platforms organise their content through automated systems (i.e. selective exposure).[101] These options can include filters for certain types of content or topics rather than specific users or groups. This also happened in the atomic world where individuals chose which kind of media outlets they want to rely on when buying a newspaper or watching television. This type of personalisation can also be beneficial for users since it leaves in the hands of individuals the possibility to choose their degree of exposure.[102] On the opposite, pre-selected personalisation is driven not only by online platforms but also exogenous factors like the goal to reach a new advertising strategy required by the market. Therefore, algorithmic accountability and transparency play a critical role in increasing users' autonomy and reduce the fragmentation of the public sphere.[103]

The challenges of content moderation could lead to the debasement of information pluralism in the digital environment. Public actors are no longer the only source of concern in the (algorithmic) marketplace of ideas. Instead of a democratic and decentralised society as defined at the end of the last century, an oligopoly of private entities has emerged, controlling information and determining how people exchange it.[104] Arendt described the public domain as a place 'where men exist not merely like other living or inanimate things, but to make their appearance explicitly' (i.e. the 'space of appearance').[105] Nonetheless, this space is not stable but highly dependent on the performances of deeds or the utterance of words. Indeed, 'unlike the spaces which are the work of our hands, it does not survive the actuality of the movement which brought it into being, but disappears not only with the dispersal of men – as in the case of great catastrophes when the body politic of a people is destroyed – but with the disappearance or arrest of the activities

[97] Micheal Schudson, 'Was There Ever a Public Sphere? If So, When? Reflections on the American Case' in John Calhoun (ed.), *Habermas and the Public Sphere* 143 (MIT Press 1992).
[98] Marshall McLuhan, *Understanding Media. The Extensions of Man* (MIT Press 1994).
[99] Neil Thurman and Steve Schifferes, 'The Future of Personalization at News Websites: Lessons from a Longitudinal Study' (2012) 13(5-6) Journalism Studies 775.
[100] Frederik J. Zuiderveen Borgesius and others, 'Should we Worry about Filter Bubbles?' (2016) 5(1) Internet Policy Review <https://policyreview.info/node/401/pdf> accessed 12 March 2020.
[101] Natalie J. Stroud, 'Polarization and Partisan Selective Exposure' (2010) 60(3) Journal of Communication 556.
[102] Natalie Helberger, 'Diversity by Design' (2011) 1 Journal of Information Policy 441.
[103] Nikolas Diakopoulos, 'Algorithmic Accountability. Journalistic Investigation of Computational Power Structures' (2014) 3 Digital Journalism 398.
[104] Martin Moore and Damian Tambini (eds), *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).
[105] Hannah Arendt, *The Human Condition* (University of Chicago Press 1998).

themselves'.[106] The primary question is whether platform determinations shaping the public debate would lead to a qualitative arrest of human activities. The lack of transparency and accountability in online content moderation frustrates the exercise of freedoms in the public sphere encouraging to rethink the role of freedom of expression as negative liberty in the information society. Platforms govern the flow of information online. They define, enforce, and balance the right to freedom of expression online according to their business logic as the next subsection explains.

3.2 The Logic of Moderation

Moderation can be defined as 'the screening, evaluation, categorisation, approval or removal/hiding of online content according to relevant communications and publishing policies. It seeks to support and enforce positive communications behaviour online, and to minimize aggression and anti-social behaviour'.[107] By focusing on the virtues of moderation, Grimmelman has defined this process as 'the governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse'.[108] Content moderation decisions can be entirely automated, made by humans or a mix of them. While the activities of pre-moderation like prioritisation, delisting and geo-blocking are usually automated, post-moderation is usually the result of a mix between automated and human resources.[109] This activity usually implies the use of different kinds of automated systems to manage a vast amount of information in different phases.[110] Moderation occurs before content is published (i.e. pre-moderation) or after publication (i.e. post-moderation). Precisely, post-moderation consists of the organisation of content, and it is implemented as a reactive measure to assess noticed content and as a proactive tool to actively monitor published content. Besides, removal is not the only way. For example, YouTube demonetises content by terminating any revenue sharing agreement with content provider. This process can lead be a powerful tool to silence certain speakers which rely on YouTube as a source of income. Another alternative to content removal is downranking or shadow banning. In this case, content is deprioritised in news feeds and other recommendation systems. This constitutes editorial decision on the organisation of content affecting how public discourse is shaped online. Platforms can decide whether certain content is visible and, therefore, affect its potential reach and dissemination.

These considerations only partially explain why moderation is a need for social media. As observed by Gillespie, 'moderation is not an ancillary aspect of what platforms do. It is essential, constitutional, definitional. Not only can platforms not survive without moderation, they are not

---

[106] Ibid, 199.
[107] Terry Flew and others, 'Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance' (2019) 10(1) Journal of Digital Media & Policy 33, 40.
[108] James Grimmelmann, 'The Virtues of Moderation' (2015) 17 Yale Journal of Law and Technology 42, 47.
[109] Sarah T. Roberts, 'Content Moderation' in Laurie A. Schintler and Connie L. McNeely (eds), *Encyclopedia of Big Dat*a (Springer 2017).
[110] Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951719897945> accessed 14 June 2020.

platforms without it'.[111] Moderation of online content is an almost mandatory step for social media not only to manage removal requests coming from Governments or users but also to prevent that their digital spaces turn into hostile environments due to the spread, for example, of incitement to hatred. The implementation of these systems has become necessary as a filter to protect good expressions from the massive presence of objectionable content. However, the interest of platforms is not just focused on facilitating the spread of opinions and ideas across the globe to foster freedom of expression. They aim to create a digital environment where users feel free to share information and data that can feed commercial networks and channels and, especially, attract profits coming from advertising revenues.[112] Facebook, for instance, aims to maximise the amount of time users spend in their digital spaces to collect data and information.[113] Therefore, this leads to developing addictive technologies and capture users' attention with inflammatory content and low degree of privacy.[114] In other words, the activity of content moderation is performed to attract revenues by ensuring a healthy online community, protect the corporate image and show commitments with ethic values. Within this business framework, users' data are the central product of online platforms under a logic of accumulation.[115]

If we would like to find the moment where the story of moderation legally began, probably he or she should look back to the aftermath of the Internet. The Big Bang of moderation can indeed be connected to the system of online intermediaries' liability based on a liberal regulatory approach adopted by the US and EU as described in Chapter II. As for the evolution of the universe, it took some phases to consolidate new profitable ways to profit from the online environment. It has been only with the first experiments of the processing of data and users' information for advertising that digital capitalism understood the potentialities of the digital environment.[116]

At the end of the last century, the Internet was still populated by merely passive providers offering access and hosting services. When the US Congress passed Section 230 of the CDA, the primary aim was to encourage the sharing of free expression and development of the digital environment.[117] In order to achieve this objective, the choice was to exempt computer services from liability for merely conveying third-party content. Before the adoption of the CDA, some cases had already made clear how online intermediaries would have been subject to a broad and unpredictable range of cases concerning their liability for editing third-party content.[118] Since this risk would have slowed down the development of new digital services in the aftermath of the

---

[111] Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* 21 (Yale University Press 2018).
[112] Tarleton Gillespie, 'Regulation of and by Platforms' in Jean Burgess, Alice E. Marwick and Thomas Poell (eds), *The SAGE Handbook of Social Media* 254 (Sage 2018).
[113] Adam Alter, *Irresistible: The Rise of Addictive Technology and the Business of Keeping us Hooked* (Penguin Press 2017).
[114] Emily Bell and Taylor Owen, 'The Platform Press: How Silicon Valley Reengineered Journalism' Tow Centre for Digital Journalism (29 March 2017) <https://www. cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php> accessed 2 October 2020.
[115] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75.
[116] Zuboff (n 92).
[117] Annemarie Bridy, 'Remediating Social Media: A Layer-Conscious Approach' (2018) 24 Boston University Journal of Science & Technology Law 193.
[118] 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. May 24 1995).

Internet, online intermediaries have been encouraged to grow and develop their business under the protection of the Good Samaritan rule.[119] Similarly, the DMCA introduced in 1997 allows online intermediaries not to be held liable for hosting unauthorised copyright works.[120] Nevertheless, unlike the CDA, the DMCA does not provide an absolute exemption but shields online intermediaries from liability according to certain conditions.[121] Likewise, in the Union, the e-Commerce Directive exempts hosting providers from liability for third-party content, provided that they remove or disable online content once they become aware of its unlawful nature.[122] The online platforms' awareness, which can result, for example, by the notice submitted by public actors or users, triggers the responsibility of online platforms to remove content. Therefore, even within the European framework, online platforms are not liable for third-party content, provided that they perform their activities in a passive way and comply with the conditions applying to the exemption of liability.[123]

At that time, there were no large corporations exercising powers in the digital environment. This is because these laws contribute to creating online platforms' business models. Several scholars have underlined how this political choice has led platforms to exploit the legal framework to their advantage. According to Pasquale, online platforms try to avoid regulatory burdens by relying on the protection recognised by the First Amendment, while, at the same time, they claim immunities as passive conduits for third-party content.[124] Likewise, Citron and Norton observe how social media 'not only are free from First Amendment concerns as private actors, they are also statutorily immunized from liability for publishing content created by others as well as for removing that content'.[125] As Tushnet underlined, Section 230 'allows Internet intermediaries to have their free speech and everyone else's too'.[126]

Notwithstanding several social media exploit rhetoric statements advocating to represent a global community and enhance free speech transnationally,[127] however, online platforms need to moderate content to protect their business interests. As observed by Roberts, 'videos and other material have only one type of value to the platform, measured by their ability to either attract users and direct them to advertisers or to repel them and deny advertisers their connection to the

[119] Zeran v Am. Online, Inc. 129 F.3d 327, 330 (4th Cir. 1997). Davis S. Ardia, 'Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act' (2010) 43 Loyola of Los Angeles Law Review 373.
[120] Digital Millenium Copyright Act (1997).
[121] Ibid, Section 512(c).
[122] 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. See Art 14.
[123] Ibid, Recital 42.
[124] Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487.
[125] Danielle Keats Citron and Helen L. Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age' (2011) 91 Boston University Law Review 1436, 1439.
[126] Rebecca Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment' (2008) 76 The George Washington Law Review 986, 1002.
[127] Mark Zuckerberg, 'Building Global Community' Facebook (16 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/> accessed 14 February 2020.

user'.[128] An eventual escape of users because of the dissemination of content like terrorism and hate could severely harm advertising revenues.

Other incentives are still linked to profit but come from concerns relating to corporate identity and reputation. For instance, online platforms aim to maintain control over the enforcement of their community guidelines and agreements to demonstrate that they act responsibly by complying with government requests relating to specific content like terrorist expressions. This content moderation paradox explains why, on the one hand, social media commit to protecting free speech, while, on the other hand, they moderate content regulating their communities for business purposes. Therefore, one of the primary issues concerns the compatibility between their private interests and public values.[129]

This situation is not only the result of the complexity of content moderation systems but also the 'logic of opacity'.[130] Platforms are interested in pursuing their depoliticisation to escape from their social responsibilities coming from their key social functions. As argued by Roberts, 'yet the process is obscured by a social media landscape that tacitly, if not explicitly, trades on notions of free circulation of self-expression, on the one hand, and a purported neutrality, on the other, that deny the inherent gatekeeping baked in at the platform level by both its function as an advertising marketplace and the systems of review and deletion that have, until recently, been invisible to or otherwise largely unnoticed by most users'.[131]

To achieve this purpose, a critical piece of the moderation logic consists of the use of artificial intelligence systems to moderate content. Platforms rely on automated technologies to cope with the amount of content uploaded by users whose non-automated management would require enormous costs in terms of human, technological and financial resources.[132] Klonick has underlined the creation of a content moderation bureaucracy made of the work of humans and machines according to internal guidelines.[133] If, on the one hand, content moderation constitutes a valuable resource (and burden) for social media, on the other hand, the use of automated technologies for moderating content on a global scale challenges the protection of freedom of expression in the digital environment with effects extending far beyond domestic boundaries.[134] The information uploaded by users is processed by automated systems that define (or at least suggest to human moderators) content to remove in a bunch of seconds according to non-transparent standards and without providing the user access to any remedy against a specific decision. It would not be possible to talk about content moderation online without considering to what extent algorithms are widely used for organising, filtering, and removal procedures.[135]

The process (and the logic) of moderation is based on automated or semi-automated systems.[136] Decisions about users' expressions are left to the discretion of machines (and

---

[128] Sarah T. Roberts, 'Digital detritus: "Error" and the Logic of Opacity in Social Media Content Moderation, (2018) 23(3) First Monday <https://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/8283/6649> accessed 28 July 2019.
[129] José van Dijck and others, *The Platform Society: Public Values in a Connective World* (Oxford University Press 2018).
[130] Roberts (n 128).
[131] Ibid.
[132] Gorwa, Binns and Katzenbach (n 110).
[133] Klonick (n 5).
[134] Balkin (n 11); James Grimmelmann, 'Speech Engines' (2014) 98 Minnesota Law Review 868.
[135] Jennifer M. Urban and others, *Notice and Takedown in Everyday Practice* (American Assembly 2016).
[136] Ben Wagner, *Global Free Expression: Governing the Boundaries of Internet Content* (Springer 2016).

unaccountable moderators) operating on behalf of online platforms.[137] These procedures govern all the phase of content in the online platforms' environment from indexation, organisation, filtering, recommendation and, eventually, removal of expressions and accounts. Scholars have underlined how these companies also rely on human intervention.[138] Still, there is who supports that this is not the solution for digital firms like Facebook due to the high amount of content to moderate.[139]

The pandemic season has amplified these concerns and showed how the implementation of artificial intelligence to moderate content contributes to spreading disinformation.[140] The decision of Google and Facebook to limit the process of human moderation has affected the entire process with the result that different accounts and content have been automatically suspended even if there was no reason to remove.[141] Although the cooperative efforts of platforms to fight this situation,[142] the pandemic has underlined not only how content moderation challenges users' rights, in this case, leading to the spread of disinformation in a time where reliance over good health information has been critical.[143] This global health emergency has provided further clues concerning the role of online platforms as essential facilities or public utilities in the information society.[144]

Within this framework, it is worth stressing that content moderation is not only a necessity for online platforms but also a way for Governments to enforce public policies online. Public bodies need to rely on online platforms to cope with terrorism, disinformation or hate speech. Governments could potentially enforce their policies online. Nonetheless, it is a matter of technical capabilities and resources. It is indeed easier to regulate or even rely on gatekeepers (e.g. telco or online platforms) to address illicit users' behaviours when we are dealing with thousands of unlawful content across multiple jurisdictions without considering that some of the alleged wrongdoers could also be artificial like bots. As examined in Chapter III, governments and online platforms can profit much more from the benefits of an indivisible handshake rather

[137] Barrett (n).
[138] Roberts (n); Paško Bilić, 'Search Algorithms, Hidden Labour and Information Control' (2016) 3(1) Big Data & Society 1
[139] Jessica Lessin, 'Facebook Shouldn't Fact Check. New York Times', The New York Time (29 November 2016) <https://www.nytimes.com/2016/11/29/opinion/facebook-shouldnt-fact-check.html> accessed 2 March 2020.
[140] Common position of European Commission and Consumer Protection Cooperation Network 20 March 2020 on stopping scams and tackling unfair business practices on online platforms in the context of the Coronavirus outbreak in the EU (20 March 2020) <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/cpc_common_position_covid19.pdf> accessed 2 July 2020.
[141] Elizabeth Dwoskin and Nitasha Tiku, 'Facebook Sent Home Thousands of Human Moderators due to the Coronavirus. Now the Algorithms are in Charge' The Washington Post (24 March 2020) < https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/> 16 June 2020.
[142] See, e.g., joint industry statement of 17 March 2020 of Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter and YouTube on working together to combat misinformation (16 March 2020) <https://about.fb.com/news/2020/06/coronavirus/> accessed 2 July 2020.
[143] Tobias R. Keller and Rosalie Gillett, 'Why is it so Hard to Stop COVID-19 Misinformation Spreading on Social Media?' The Conversation (13 April 2020) <https://theconversation.com/why-is-it-so-hard-to-stop-covid-19-misinformation-spreading-on-social-media-134396> accessed 16 June 2020.
[144] Dan Schiller, 'Reconstructing Public Utility Networks: A Program for Action' (2020) 14 International Journal of Communication 4989.

than from regulation.[145] On the one hand, regulating content moderation would decrease the flexibility to use online platforms as instruments of public surveillance or collection of data, transforming platforms' digital spaces from an area for fostering free expression in a cage for liberties. On the other hand, online platforms aim to maintain a cooperative approach to protect their freedoms to run their business and avoid high regulatory pressures.

Therefore, public/private cooperation is inside the logic of moderation, even if it could seem irrelevant or even invisible at first glance. This is also the reason why the regulation of online platforms has not changed until recently and just in Europe. Balkin has underlined that 'public/private cooperation—or cooptation—is a natural consequence of new-school speech regulation'.[146] Likewise, Reidenberg clarified as one of the systems to encore public policies online consists of not only regulating the architecture of the digital environment but also relying on online intermediaries.[147] Within this framework, governing by proxy online could be almost a mandatory step for public actors to address unlawful content online even if it raises high risks for fundamental rights and liberties as the next subsections underline in the case of freedom of expression.

3.3 Private Enforcement of Freedom of Expression

The mix of digital liberalism and predictive instruments is the reason which has led us to address this troubling scenario for freedom of expression in the digital environment. The legal immunity mixed with profiling technologies for moderating content constitutes a green light for online platforms to freely choose which values they want to protect and promote, no matter if democratic or anti-democratic and authoritarian. This is a perfect environment to profit without responsibility. Since online platforms are private businesses, they would likely focus on minimising economic risks rather than ensuring a fair balance between fundamental rights in the digital environment. In other words, the system of online intermediaries' liability has indirectly entrusted online platforms with the role of moderating content and encourage them to develop new profitable automated systems to organise, select and remove content based on a standard of protection of free speech influenced by business purposes.

The scope of online platforms' power can be better understood by focusing on how these actors set and enforce their internal rules of moderation after balancing conflicting interests. When organising, recommending or removing, platforms make decisions on which kind of speech should be protected or fostered.[148] This is evident in the process of removal reflecting some characteristics of the powers traditionally vested in public authorities as underlined in Chapter III. Human moderators refer to community guidelines or internal documents as 'private legal basis'

[145] Michael D. Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Virginia Journal of Law & Technology 6. See, also, Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 Brookling Law Review 105.
[146] Jack M. Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296, 2305.
[147] Joel R Reidenberg, 'States and Internet enforcement' (2004) 1 University of Ottawa Law & Technology Journal 213.
[148] Hannah Bloch-Webba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU Law Review 27.

to remove content. Social media usually provide ToS and community guidelines where they explain users the acceptable conducts and content, creating 'a complex interplay between users and platforms, humans and algorithms, and the social norms and regulatory structures of social media'.[149]

However, these community rules do not necessarily represent the reality of content moderation. Facebook, for example, relies on internal guidelines which users cannot access and whose drafting process is unknown.[150] According to Klonick, Facebook's content moderation is 'largely developed by American lawyers trained and acculturated in American free-speech norms, and it seems that this cultural background has affected their thinking'.[151] Whatever American or European values are at stake, this process is far from being close to any democratic value. Besides, the use of internal guidelines which are not publicly disclosed, leads to looking at this process more as an authoritarian determination than a democratic expression.

The situation is even more complicated when internal standards are solely implemented by machines which translate top-down rules in an enforceable series of code, defining another layer of complexity in the moderation of expressions. From a technical perspective, the opacity of content moderation also derives from the implementation of machine learning techniques subject to the 'black box' effect.[152] On the one hand, algorithms can be considered as technical instruments facilitating the organisation of online content. Nevertheless, on the other hand, such technologies can constitute opaque self-executing rules, obviating any human control with troubling consequences for democratic values such as transparency and accountability. This mix of human and machines definition of freedom of expression constitutes the basis for enforcing decisions which are the results of a balance between conflicting interests. Whatever content users' or Government flag or signal to online platforms, it is because that expression is considered as a violation of a right (e.g. hate speech) or in conflict with public legitimate interests (e.g. national security). Taking as example the case of hate speech, it is worth observing how this concept coming from an understanding of rights and freedom as public values is then mediated by the private determinations of human moderators or machines. This process then leads to the hybridisation of freedom of expression where traditional dichotomies like public/private or human/machine merge in a unique soul.

Within this framework, the lack of any users' rights or remedy leads online platforms to exercise the same discretion of absolute power over its community. Despite the fundamental role of online platforms in establishing the standard of free speech and shaping democratic culture on a global scale,[153] the information provided by these companies about content moderation is opaque or lawless, thus, threatening the rule of law.[154] Online platforms are free to decide how to

[149] Kate Crawford and Tarleton Gillespie, 'What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint' (2016) 18 New Media & Society 410, 411.
[150] Max Fisher, 'Inside Facebook's Secret Rulebook for Global Political Speech' New York Times (27 December 2018) <https://www.nytimes.com/2018/12/27/world/facebook-moderators.html> accessed 20 June 2020.
[151] Klonick (n 5), 1622.
[152] Frank Pasquale, *The Black Box Society. The Secret Algorithms that Control Money and Information* (Harvard University Press 2015).
[153] Marvin Ammori, 'The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter' (2014) 127 Harvard Law Review 2259.
[154] Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019).

show and organise online content according to predictive analysis based on the processing of users' data. In other words, although, at first glance, social media foster freedom of expression by empowering users to share their opinion and ideas cross-border, however, the high degree of opacity and inconsistency of content moderation frustrates democratic values.

Content moderation does not only constitute an autonomous set of technical rules to control digital spaces but also contributes to defining the standard of protection of fundamental rights online, thus, shaping the notion of public sphere and democracy. This situation leads to 'mathematising the law' since the concept of legality is defined by a mere algorithmic calculation. The power of online platforms to shape the scope of protection of rights lies mostly in their ability to mathematically materialise abstract notions through digital means. Since artificial intelligence technologies are always becoming more pervasive in online content moderation, the opacity of these technologies raises legal (and ethical) concerns for democracy.[155] Individuals are increasingly surrounded by technical systems influencing their decisions without the possibility to understand or control this phenomenon.[156] In other words, notwithstanding the Internet has allowed users to access different types of information, the mediation of automated technologies leads users to participate in what Cohen defines a 'modulated democracy'.[157]

4. The First Steps of Digital Constitutionalism

In the process of content moderation, users are not only subject to the private determinations of online platforms on freedom of expression but, more importantly, they cannot generally rely on any legal right concerning the moderation of their content. In other words, as observed by Myers West, 'they are exactly the kinds of users who make up the kind of "town square," "global village," or "community" that these platforms themselves say they seek to cultivate—but current content moderation systems do not give them much opportunity to participate or grow as citizens of these spaces'.[158]

From an international perspective, both the Manila principles on intermediary liability and the IGF Dynamic Coalition on Platform Responsibility propose an approach towards the proceduralisation of content moderation.[159] Similarly, the Santa Clara principles on Transparency and Accountability in Content Moderation try to suggest the adoption of due process safeguards regarding how content moderation should be performed and what rights users can rely on in the context of this process.[160] Article 19 has proposed the creation of social media councils based on a self-regulatory and multi-stakeholder system of accountability for content moderation

[155] Brent D. Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679> accessed 28 May 2020.
[156] Paul Nemitz, 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) 376 Royal Society Philosophical Transactions A.
[157] Julie E. Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904.
[158] Sarah Myers West, 'Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms' (2018) 20(11) New Media & Society 4380. See Trevor Puetz, 'Facebook: The New Town Square' (2014) 44 Southwestern Law Review 385.
[159] Manila Principles on Intermediary Liability (2017) and the DCPR Best Practices on Platforms' Implementation on the Right to Effective Remedy <https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4905/1550> accessed 16 June 2020.
[160] Santa Clara Principles on Transparency and Accountability in Content Moderation (2018) < https://santaclaraprinciples.org/> accessed 16 June 2020.

complying with international human rights' standards.[161] Likewise, in 2019, Facebook has launched its oversight board.[162] At the same time, Twitter set an independent research group whose task is to develop standards for content moderation.[163]

However, despite the relevance of this proposal, we are still dealing with discretionary and voluntary mechanisms. The lack of any binding force of this system leaves online platforms free to decide whether to participate in this mechanism or formally comply with these standards while maintaining their internal rules of procedures. At the same time, the UN Special Rapporteur for Freedom of Expression, David Kaye, underlined the increasing pressure on private actors to comply with international human rights law when moderating online content.[164] According to the Special Rapporteur, since social media exercise regulatory functions in the digital environment, these private actors should refer to the existing international human rights law regime when setting their standard for content moderation.[165] International human rights law could help platforms to apply a universal reference in their activities of content moderation but still there are challenges concerning the promise of human rights law in content moderation.[166]

As already underlined, since online platforms are private actors, they are not obliged to respect human rights since international human rights law vertically binds only State actors with the result that the governance of online platforms is based on fragmented national and regional laws as well as soft-regulatory efforts.[167] The same consideration extends to fundamental rights since constitutional provisions bind just public actors to respect them even if there could be some cases where fundamental rights horizontally apply in the relationship between private actors.[168] Despite the role of self-regulation and corporate social responsibility in building a shared global framework which could overcome any regulatory vacuum,[169] the remedies voluntarily provided

[161] Article 19, 'The Social Media Councils: Consultation Paper' (2019) <https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf> accessed 8 October 2019.
[162] Kate Klonick, 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) 129 Yale Law Journal 2418; Evelyn Douek, 'Facebook's "Oversight Board:" Move Fast with Stable Infrastructure and Humility' (2019) 21(1) North Carolina Journal of Law and Technology 1.
[163] Katie Paul and Munsif Vengattil, 'Twitter Plans to Build "Decentralized Standard" for Social Networks' *Reuters* (11 December 2019) <https://www.reuters.com/article/us-twitter-content/twitter-plans-to-build-decentralized-standard-for-social-networks-idUSKBN1YF2EN> accessed 2 July 2020.
[164] David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019).
[165] Report of the Special Rapporteur to the Human Rights Council on online content regulation, A/HRC/38/35 (2018); See, also, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348 (2018); Guiding Principles on Business and Human Rights (2011).
[166] Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of A Human Rights based Approach to Content Moderation' (2020) 43(4) Fordham Journal of International Law 939.
[167] Jennifer Grygiel and Nina Brown, 'Are Social Media Companies Motivated to Be Good Corporate Citizens? Examination of the Connection Between Corporate Social Responsibility and Social Media Safety' (2019) 43 Telecommunications Policy 445.
[168] Some constitutions around the world (e.g. South Africa) horizontally extends the application of fundamental rights in the relationship between private actors. In other case, horizontal application is not the result of a direct constitutional provision but the result of judicial interpretation.
[169] Rolf H. Weber, 'Corporate Social Responsibility as a Gap-Filling Instrument', in Andrew P. Newell (ed.). *Corporate Social Responsibility: Challenges, Benefits and Impact on Business* 87 (Nova 2014).

by online platforms are highly fragmented and left to their discretion.[170] Moreover, the differences between (public available) community guidelines and (private hidden) internal policy as well as the opacity about the use of automated systems in content moderation create a grey area of cases where organisation, recommendation and removal of content are set outside any democratic control.

While, in the US, the legal framework has not changed in the last twenty years, apart from the recent amendments introduced to Section 230 CDA,[171] and the executive order on preventing online censorship adopted in 2020,[172] the Union has started to pave the way towards a new regulatory season of online content moderation, as stressed in Chapter II. The European objectives to 'protect core values' while increasing 'transparency and fairness for maintaining user trust and safeguarding innovation' could be considered the political manifesto of the new European approach.[173] Such a shift towards 'wider responsibility' is not a mere political decision but the expression of the first steps of digital constitutionalism.[174]

We have already underlined how the Directive on Copyright in the Digital Single Market ('Copyright Directive'),[175] the amendments to the Audiovisual Media Service Directive,[176] and the proposal for a Regulation on tackling the dissemination of terrorist content online ('Regulation on Terrorist Content'),[177] have constituted a first turning point in online content moderation, requiring online platforms to establish transparent and accountable mechanisms. The Copyright Directive is the only legal instrument at the European level introducing a special regime derogating the system established by the e-Commerce Directive for online platforms' liability while introducing users' safeguards.[178] Likewise, the Regulation on Terrorist Content, which aims to establish a clear and harmonised legal framework to prevent the misuse of hosting services (online platforms) for the dissemination of terrorist content online, is another interesting example of users' rights in online content moderation.[179]

---

[170] IGF Dynamic Coalition, 'Best Practices on Platforms' Implementation of the Right to an Effective Remedy' (2018) <https://www.intgovforum.org/multilingual/content/dcpr-best-practices-on-due-process-safeguards-regarding-online-platforms'-implementation-of> accessed 7 August 2019.

[171] See the Stop Enabling Sex Traffickers Act (SESTA) and the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) adopted in 2018.

[172] Executive Order on Preventing Online Censorship (28 May 2020) <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> accessed 8 June 2020.

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

[174] Ibid.

[175] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130/92.

[176] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018) OJ L 303/69.

[177] 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)).

[178] Copyright Directive (n 175), Art 17.

[179] Regulation on Terrorist Content (n 177), Art 1. See Joris van Hoboken, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications' (2019) Transatlantic Working Group on Content Moderation Online and Freedom of Expression

These two measures are part of a broader strategy of the Union to foster accountability and transparency in online content moderation. Just to mention two examples, it would be enough to refer to the Code of Conduct on Countering Illegal Hate Speech Online and the Code of Practice on Online Disinformation,[180] resulting from the Communication on Tackling Online Disinformation and, especially, the Communication on tackling illegal content online,[181] then implemented in the Recommendation on measures to effectively tackle illegal content online.[182]

The approach of the Union in this field shows a shift from a liberal approach in online content moderation to transparency and accountability obligations and recommendations. Rather than just focusing on content regulation, the European approach focuses on introducing procedural safeguards for users to dismantle the logic of opacity. The Digital Services Act would be another opportunity to complete this framework systematically.

In the meantime, in *Eva Glawischnig-Piesczek v Facebook Ireland Limited*,[183] the ECJ has contributed to providing guidance in the process of content moderation in a case involving the removal of identical and equivalent content. The ECJ underlined the role of social media in promoting the dissemination of information online, including illegal content. In this case, national judge's orders of removal or blocking of identical content do not conflict with the monitoring ban established by the e-Commerce directive.[184] As the AG Szpunar underlines, an order to remove all identical information does not require 'active non-automatic filtering'.[185] The ECJ addressed the question concerning the removal of 'equivalent' content. According to the court, in order to effectively cease an illegal act and prevent its repetition, the order of the national judge has to be able to also extend to 'equivalent' content defined as 'information conveying a message the content of which remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality'.[186] Otherwise, users would only access a partial remedy that could lead to resorting to an indefinite number of appeals to limit the dissemination of equivalent content.[187]

<https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf> accessed 29 July 2019; Aleksandra Kuczerawy, 'The Proposed Regulation on Preventing the Dissemination of Terrorist Content Online: Safeguards and Risks For Freedom Of Expression' (2018) CITIP paper for the Center for Democracy and Technology, <https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf> accessed 29 July 2019; Joan Barata, 'New EU Proposal on the Prevention of Terrorist Content Online' (2018) CIS Stanford Law <https://cyberlaw.stanford.edu/files/publication/files/2018.10.11.Comment.Terrorism.pdf> accessed 26 July 2019.

[180] Code of conduct on countering illegal hate speech online (2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300> accessed 21 October 2019; Code of practice on disinformation (2018) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 25 October 2019.

[181] 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.

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

[183] Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited (2019).

[184] Ibid, 37.

[185] Opinion of Advocate General in Eva Glawischnig-Piesczek v Facebook Ireland Limited (4 June 2019), 61.

[186] C-18/18 (n 183), 39.

[187] Ibid, 41.

However, such an extension is not unlimited. Indeed, the ECJ reiterated that the ban on imposing a general surveillance obligation established by the e-Commerce Directive is still the relevant threshold for Member States' judicial and administrative orders. If, on the one hand, the possibility of extending the orders of the national authorities to equivalent content aims to protect the victim's honour and reputation, on the other hand, such orders cannot entail an obligation for the hosting provider to generally monitor information to remove equivalent content. In other words, the ECJ defined a balance between, on the one hand, the freedom of economic initiative of the platform, and, on the other, the honour and reputation of the victim. The result of such a balance, therefore, leads to reiterate that the national orders of the judicial and administrative authorities have to be specific without being able to extend to the generality of content.

In order to balance these conflicting interests, the ECJ provided other conditions applying to equivalent content. Precisely, expressions have to contain specific elements duly identified by the injunction like 'the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal'.[188] Under these conditions, the protection granted to the victim would not constitute an excessive obligation on the hosting provider since its discretion is limited to certain information without leading to general monitoring obligation that could derive from an autonomous assessment of the equivalent nature of the content. If, on the one hand, the ECJ clarified how platforms should deal with users' requests for removal of identical and equivalent content, nonetheless, even in this case, the court did not define transparency and accountability safeguards in the process of content moderation.

These crucial steps of digital constitutionalism have not solved the asymmetry of power in the field of content. Users and online platforms still face challenges raised by legal fragmentation in this field. There is not a unitary framework of users' rights or remedies without stressing the fact that Member States enjoy margins of discretion in implementing such safeguards. Besides, safeguards in online content moderation have not been introduced horizontally to cover all content and situation. The Union has maintained a vertical approach based on specific categories of content (e.g. copyright content), and there is no coordination between different safeguards. The fragmentation of content moderation processes can lead to serious consequences for the freedom to conduct business of online platforms and, as a consequence, this uncertainty could produce chilling effects for users' freedom of expression.

Therefore, it is time to focus on how the new phase of European digital constitutionalism can provide instruments to address the imbalance of power between users and online platforms in the field of content. There are two ways addressed in the next sections, respectively looking at the horizontal effect doctrine and a new understanding of media pluralism online through a regulatory framework of content moderation.

5. Horizontal Effect as Filling Regulatory Gaps?

Within this troubling framework for democratic values in the algorithmic society, the question would be whether European constitutional law already owns the instruments to react without regulatory intervention. Whereas proposing a regulatory solution would be a largely traditional

[188] Ibid, 45.

approach, it is necessary to step back and wonder the role of constitutional law in content moderation. Even if, in Europe, lawmakers have seemed to be prone to regulate online platforms, it should not be neglected the interest, on the one hand, of public actors to monitor online activities and enforce public policies online. On the other hand, online platforms aim to maintain their freedom to conduct business outside regulatory interferences. This apparently unrelated but converging interests leads to invisible cooperation between public and private actors, thus, creating a powerful brake to regulatory intervention.[189] Such a situation could lead to a potential conflict of interest of political power which should face how to regulate online platforms while maintaining cooperation.

To overcome such political impasse, one of the few ways to move further is to look at judicial power and independence. In other words, it would be possible to rely on courts to ensure that the protection of fundamental rights is not locked down between political and business interests but is interpreted within the evolving information society. This approach would lead to wondering to what extent the horizontal effect doctrine of fundamental rights in Europe could be a solution to remedy the imbalance of power between users and online platforms exercising private powers on freedom of expression online.

The horizontal doctrine would indeed promise to go beyond the public/private division extending constitutional obligations even to the relationship between private actors (i.e. platform/user). Unlike the liberal spirit of the vertical approach, this theory rejects a rigid separation where constitutional rules apply vertically only to public actors to ensure the liberty and autonomy of private actors. Put another way, the horizontal doctrine is concerned with the issue of whether and to what extent constitutional rights can affect the relationships between private actors. As observed by Gardbaum, '[t]hese alternatives refer to whether constitutional rights regulate only the conduct of governmental actors in their dealings with private individuals (vertical) or also relations between private individuals (horizontal)'.[190] The horizontal effect can result from constitutional obligations on private parties to respect fundamental rights (i.e. direct effect) or their application through judicial interpretation (i.e. indirect effect). Only in the first case, a private entity would have the right to rely directly on constitutional provisions to claim the violation of its rights vis-à-vis other private parties.[191] There is also a third (indirect) way through the positive obligations for States to protect human rights like in the case of Convention.[192]

The horizontal application of fundamental rights could constitute a limitation to the expansion of power by social subsystems. According to Teubner, the emergence of transnational regimes shows the limits of constitutions as means of regulation of the whole society since social sub-systems develop their own constitutional norms.[193] Therefore, the horizontal effects doctrine can

[189] Birnhack and Elkin-Koren (n 145).
[190] Stephen Gardbaum, 'The Horizontal Effect of Constitutional Rights' (2003) 102 Michigan Law Review 388.
[191] John H. Knox, 'Horizontal Human Rights Law' (2008) 102(1) American Journal of International Law 1.
[192] Daniel Augenstein and Lukasz Dziedzic, 'State Responsibilities to Regulate and Adjudicate Corporate Activities under the European Convention on Human Rights' (2017) EUI Working papers < https://cadmus.eui.eu/bitstream/handle/1814/48326/LAW_2017_15.pdf?sequence=1&isAllowed=y> accessed 1 October 2020.
[193] Gunther Teubner 'The Project of Constitutional Sociology: Irritating Nation State Constitutionalism' (2013) 4 Transnational Legal Theory 44.

be considered a limit to self-constitutionalising private regulation. As a result, if the horizontal effect of fundamental rights is purely considered a problem of political power within society, an approach which excludes its application would hinder the teleological approach behind the horizontal doctrine, the aim of which is to protect individuals against unreasonable violation of their fundamental rights vis-à-vis private actors. As Tushnet underlined, if the doctrine of horizontal effect is considered 'as a response to the threat to liberty posed by concentrated private power, the solution is to require that all private actors conform to the norms applicable to governmental actors'.[194]

Nonetheless, the horizontal application of fundamental rights does not apply in the same way across the Atlantic. Within the US framework, the Supreme Court has usually applied the vertical approach where the application of the horizontal approach, known in the US as the 'state action doctrine', would be considered the exception.[195] The First Amendment, and, more in general, US constitutional rights,[196] lack horizontal effect not only *in abstracto* but also in relation to online platforms. Even if scholars have tried to propose new ways to go beyond such a rigid verticality,[197] the Supreme Court has been clear about the limits of this doctrine when addressing the possibility that a non-profit corporation designated by New York City to run a public access television network limit users' speech.[198] In an ideological 5-4 ruling, the court rejected the idea that the TV station in question could be considered a state actor, and, therefore, there was no reason to focus on the violation of the First Amendment. Notwithstanding this case concerned public access channels, the property-interest arguments could have a broad impact in the information society, precisely on the protection of online platforms' speech. This would lead towards Balkin's view when he warns about the limit of 'judge-made doctrines' of First Amendment.[199]

The horizontal extension of fundamental rights is less rigid in the European environment.[200] A possible explanation for such differences could be the impact of social democratic openness of Member States and the European area which is far from the liberal approach of the US framework. According to Tushnet, states which are more oriented to develop welfare systems and provide

---

[194] Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' 1(1) International Journal of Constitutional Law 79.

[195] Shelley v Kraemer 334 US 1 (1948). Mattias Kumm and Victor Ferreres Comella, 'What Is So Special about Constitutional Rights in Private Litigation? A Comparative Analysis of the Function of State Action Requirements and Indirect Horizontal Effect' in Andras Sajó and Renata Uitz (eds), T*he Constitution in Private Relations: Expanding Constitutionalism* 265 (Eleven 2005); Mark Tushnet, 'Shelley v. Kraemer and Theories of Equality' (1988) 33 New York Law School Law Review 383.

[196] The prohibition on slavery as provided for by the Thirteenth Amendment applies to public and private actors. Gardbaum (n 190) 388; George Rutherglen, 'State Action, Private Action, and the Thirteenth Amendment' (2008) 24(6) Virginia Law Review 1367.

[197] Jonathan Peters, 'The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms' (2018) 32 Berkeley Technology Law Journal 988; Lyrissa B. Lidsky, 'Public Forum 2.0' (2011) Boston University Law Review 1975; Paul S Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 University of Colorado Law Review 1263.

[198] Manhattan Community Access Corp. v. Halleck, No. 17-1702, 587 U.S. ___ (2019).

[199] Jack M. Balkin, 'The Future of Free Expression in a Digital Age' (2009) 36 Pepperdine Law Review 427, 443-444.

[200] Regarding the horizontal effect of fundamental rights in the EU framework, see Eleni Frantziou, *The Horizontal Effect of Fundamental Rights in the European Union. A Constitutional Analysis* (Oxford University Press 2019); Sonya Walkila, *Horizontal Effect of Fundamental Rights in EU Law* (European Law Publishing 2016).

social rights in their constitutions more readily apply the horizontal effect doctrine.[201] This position should not surprise since it is the natural consequence of how rights and freedoms are conceived in welfare States. Positive and programmatic nature of some constitutional rights lead to a broader role for lawmakers but, especially, for courts to define the limits of these rights. It is not by chance that, in the European framework, the doctrine of the horizontal effect has found its application in the field of labour law.[202]

The European horizontal effect doctrine is far from being locked just in the field of social rights.[203] Traditionally, the effects of the rights recognised directly under EU primary law have been capable of horizontal application. The ECJ has applied both the horizontal effect and the positive obligation doctrines regarding the four fundamental freedoms and general principles.[204] In the *Van Gend En Loos* case, the ECJ stated: 'Independently of the legislation of Member States, Community law not only imposes obligations on individuals but is also intended to confer upon them rights which become part of their legal heritage'.[205] This definition remained unclear until the court specified its meaning in *Walrave* ,[206] which, together with *Bosman,*[207] and *Deliege,*[208] can be considered the first acknowledgement of the horizontal effect of the EU fundamental freedoms.[209]

Likewise, since the Charter acquired the same legal value of Treaty,[210] judicial activism has also been extended to the Charter.[211] Recently, in *Egenberger*,[212] the ECJ extended horizontal application to the right of non-discrimination and the right to an effective remedy and to a fair trial, respectively enshrined in Articles 21 and 47 of the Charter, in a case involving compensation for discrimination on the grounds of religion suffered in a recruitment procedure. Likewise, in *Bauer*,[213] the court went even further. The ECJ did not only extend horizontal effects to the right to limitation of maximum working hours as fair and just working condition,[214] but also overcame its precedents in *Association de médiation sociale,* where it rejected horizontal effects to the

[201] Tushnet (n 194).
[202] See Case 43/75 Defrenne v Sabena (No 2) (1976). More recently, Case C-555/07 Kücükdeveci v Swedex (2010); Case C-144/04 Mangold v Rüdiger Helm (2005). But see Case C-176/12 Association de médiation sociale v Union locale des syndicats CGT (2014).
[203] Valeria Piccone and Oreste Pollicino (eds), *La Carta dei diritti fondamentali dell'Unione europea* (Editoriale scientifica 2018).
[204] Elena Gualco and Luisa Lourenço '"Clash of Titans". General Principles of EU Law: Balancing and Horizontal Direct Effect' (2016) 1(2) European Papers 643.
[205] Case 26/62 van Gend & Loos v Netherlands Inland Revenue Administration (1963).
[206] Case 36/74 Walrave v Association Union cycliste international (1974).
[207] Case C-415/93 Union royale belge des sociétés de football association v Bosman (1995).
[208] Case C-51/96 Deliège v Ligue francophone de judo et disciplines associées (2000).
[209] Among the other decisions, see Case C-281/98 Angonese v Cassa di Risparmio di Bolzano (2000); Case C-103/08 Gottwald v Bezirkshauptmannschaft Bregenz (2009); Case C-223/09 Dijkman v Belgische Staat (2010).
[210] Consolidated version of the Treaty on European Union (2012) OJ C 326/13, Art 6(1). Grainne De Burca and Jo B Aschenbrenner, 'The Development of European Constitutionalism and the Role of the EU Charter of Fundamental Rights' (2003) 9 Columbia Journal of European Law 355.
[211] Dorota Leczykiewicz, 'Horizontal Application of the Charter of Fundamental Rights' (2013) 38(3) European Law Review 479.
[212] Case C-414/16 Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V. (2018).
[213] Case C-569/16 Stadt Wuppertal v Maria Elisabeth Bauer and Volker Willmeroth v Martina Broßonn (2018).
[214] Charter (n 51), Art 31(2).

workers' right to information and consultation.[215] In *Bauer*, the ECJ clarified that the narrow scope of Article 51(1) does not deal with whether individuals, or private actors, may be directly required to comply with certain provisions of the Charter.[216]

With regard to the right to the freedom of expression as enshrined in the Charter,[217] the ECJ has not still provided its guidance. A literal interpretation of Article 11 of the Charter could constitute a barrier to any attempt to extend its scope of application. Likewise, Article 51(1) of the Charter seems to narrow the scope of application of the Charter to EU institutions and Member States in their implementation of EU law.[218] Brkan warned about the risk for the system of European competences relating to the introduction of a positive obligation in the field of freedom of expression to fill the legislation gap.[219] Indeed, 'in creating such a positive obligation, the CJEU would not only have to observe the principles of conferral and subsidiarity, but also pay attention not to overstep its own competences by stepping into the shoes of a legislator'.[220] This, however, has not discouraged the ECJ to underline the relevance of the right to freedom of expression online in private litigations.[221] The court underlined that 'the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued'.[222]

The reasons for an alleged lack of horizontality are not only rooted in the separation between judicial and political power but also depends on the constitutive difference between negative liberties and positive rights. As Beijer underlined, in the Union framework, there is less pressure to rely on positive obligations based on the violation of fundamental rights since obligations are horizontally translated in acts of EU law.[223] The approach of the ECJ does not surprise since the labour law field can be considered one of the primary expressions of the welfare conception. The extension of such a rule to the principle of non-discrimination aim to ensure not only formal but also substantive equality between individuals. In this framework, the right to freedom of expression is instead conceived within the framework of negative liberties which only consider public actors as a threat. In other words, it is not just a matter of literal interpretation of Article 11 of the Charter but also of theoretical distance, even if the common matrix of human dignity in

---

[215] C-176/12 (n 202), 51.
[216] C-569/16 (n 213), 87.
[217] Charter (n 51), Art 11.
[218] Ibid. According to Art 51(1): 'The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective power'.
[219] Maja Brkan, 'Freedom of Expression and Artificial Intelligence: On Personalisation, Disinformation and (Lack Of) Horizontal Effect of the Charter' SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354180> accessed 24 February 2020.
[220] Ibid.
[221] Case C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (2014); Case C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (2016).
[222] Telekabel (n 221), 56. See also Mc Fadden (n 221), 93.
[223] Malu Beijer, *The limits of Fundamental Rights Protection by the EU: The Scope for the Development of Positive Obligations* 297 (Intersentia 2017).

European constitutionalism could provide that constitutional ground to extend horizontal effects to freedom of expression.

Besides, within the complexity of the horizontal effect doctrine,[224] it is worth highlighting at least a primary drawback. Applying this doctrine extensively could lead to negative effects for legal certainty. Every private conflict can virtually be represented as a clash between different fundamental rights. The result could lead to the extension of constitutional obligations to every private relationship, thus, hindering any possibility to foresee the consequences of a specific action or omission. Fundamental rights can be applied horizontally only *ex post* by courts through the balancing of the rights in question. It cannot be excluded that this approach could be even more multifaceted in civil law countries where judges are not legally bound by precedents, but they can take their path on whether extending constitutional obligations to private litigations.[225] This process could increase the degree of uncertainty as well as judicial activism, undermining the principles of the separation of powers and the rule of law.

When framing these considerations in the field of content moderation, the horizontal effect doctrine could be a constitutional instrument to generally mitigate the exercise of private powers on freedom of expression. Nonetheless, the extension of obligations to respect constitutional rights to online platforms would raise several concerns. Firstly, extending such a doctrine would increase the power of courts in the information society. In Chapter II, the judicial activism of the ECJ has already shown the role of courts in ensuring that the protection of fundamental rights is not frustrated in the digital environment. The further empowerment of judicial over political power could lead to increasing fragmentation and uncertainty about obligations of content moderation.

The concern around judicial power could be partially overcome by limiting the application of the horizontal effect only to those cases where private actors exercise their autonomy as a result of the delegation of public functions. In the case of platforms, although these entities cannot be considered public actors *per se*, their delegated public functions to moderate content (e.g. obligation to remove illicit content in case of awareness) could be subject to the safeguards applying to the public sector (e.g. transparency). In other words, constitutional law would extend its horizontal boundaries only where public actors entrust private actors with quasi-public functions through delegation of powers.[226] Users have legitimate expectation that if a public actor has entrusted a private one to pursue a public policy, it is necessary that those private actors be held accountable for violating users' fundamental rights. On the opposite, where platforms exercise autonomous powers, a broad extension of the horizontal effect doctrine would transform these entities into public actors by default. This approach would provide users with the right to

[224] Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press 2002).

[225] The difference between common law and civil law should not be considered rigid. Nonetheless, the constitutive differences in the role of Courts deserve to be mentioned when focusing on the limits of the horizontal effect doctrine. See, generally, Paul Brand and Joshua Getzler (eds), *Judges and Judging in the History of the Common Law and Civil Law: From Antiquity to Modern Times* (Cambridge University Press 2015); Joseph Dainow, 'The Civil Law and the Common Law: Some Points of Comparison' (1966-1967) 15(3) American Journal of Comparative 419.

[226] A constitutional oriented interpretation of the responsibilities of online platforms in light of European constitutional values could mitigate platforms' discretion. In the field of the right to be forgotten, the ECJ has recognised the obligation of search engines to delist results based on the constitutional oriented interpretation of the right to privacy and data protection enshrined in the Charter.

bring claims related to violations of, for example, freedom of expression directly against platforms as entities performing delegated public functions.

At first glance, this mechanism would allow fundamental rights to become horizontally effective against the conduct or omission of actors evading their responsibilities and shielding their activities under a narrative based on freedoms and liberties. However, a closer look could reveal how empowering users to challenge online platforms could lead to a compression of the freedom to conduct business of these actors since such an approach could break the online platforms' exception of liability. Such interference could not be tolerated under a European constitutional perspective. Freedom of expression is not an absolute right with the result that its protection needs to take into account the effects over other constitutional interests like the economic freedom to conduct business of online platforms as enshrined in the Charter.

Besides, requiring online platforms not to censor content or generally avoid interferences with freedom of expression (e.g. must carry obligations) could block the process of content moderation with the result that the digital environment would be invaded by objectionable content. This would undermine not only the freedom to conduct business of online platforms which would lose advertising revenues but also democratic values online since users which would be exposed to more illicit content in the digital environment. This situation would reduce their freedom to share opinion and ideas online.

Within this framework, the horizontal effect doctrine cannot always provide a stable solution for the imbalances between public and private power in the information society. It could be a reactive remedy which would not be able to comprehensively mitigate the challenges of content moderation. This does not imply that judges could not play a critical role in protecting constitutional values from technological annihilation. On the one hand, this doctrine would perfectly match with the reactive side of European digital constitutionalism. On the other hand, it would fail to provide the other side of this constitutional season, namely a normative framework based on the injection of democratic values online to deal with private powers in the long run.

Still, there would be another chance for freedom of expression to mitigate and remedy the challenges from a European constitutional perspective. By moving from a negative to a positive dimension, it is possible to think how freedom of expression should be protected not only as negative liberty but also as a positive right. This is not a call to define the welfare of freedom of expression but to understand the role of media pluralism in the digital environment. The role of digital constitutionalism is not only to provide brand new solutions but also to reframe old categories into the new technological scenario. As the next section suggests, to avoid that the development of the digital environment remains in the hands of actors exercising significant power over constitutional rights and freedoms without pursuing public interests, it is not necessary to go beyond media pluralism but understand how to foster and promote diversity and transparency in content moderation whose characteristics are different from traditional logic.

6. Rethinking Media Pluralism Online

At this point, the remedies proposed to address the challenges of content moderation at the European level would not provide a comprehensive approach. While waiting for the proposal for the Digital Services Act, the degree of fragmentation of users' rights and the limit of a direct (or even indirect) horizontal application does not seem to provide a reliable harmonised framework

to remedy platform power and empower users in the algorithmic society. Such safeguards would lead to more legal uncertainty, thus, undermining not only fundamental rights but also the principle of the rule of law. This does not mean that the steps forward of digital constitutionalism in the field of content should be thrown away. They are surely a turning point in this field, but fragmenting content moderation would introduce more risks than advantages.

Still, beyond these measures, it is worth wondering how European constitutional law can lead to complementing these measures to remedy the current situation of the public sphere. Users enjoy a broader range of possibilities to share their ideas and opinion online in a social media environment almost free from regulatory interferences. This would look like the perfect environment to ensure the active and negative dimension of the right to freedom of expression. Social media have allowed users to share their ideas and opinions across the globe. At the same time, these actors have benefited from their private nature to ensure environment without public actors' intervention. What freedom of expression lacks in the algorithmic society is information quality, which would foster the right of users to be informed and their autonomy in a democratic society. It is not just a matter of which online platforms' activities should be regulated or how to regulate content moderation but how to legally empower users. In the algorithmic society, the primary point is how to ensure that human dignity is not frustrated by the lack of autonomy. Without self-determination, people would not be able to express their identity and consciously participate in the democratic debate. If we focused on authoritarian forms of government, human dignity could be overcome by predominant public interests since individuals' autonomy and self-determination would be substitute by the central logic of power and values. However, since we are addressing the challenges of content moderation in the Europe, whose constitutional grounds are based on the democratic principle, human dignity becomes the pillar of the entire system of the information society. Therefore, ensuring quality of access (rather than more access) is critical to foster the role of humans in a digital democratic society. In other words, this would lead to thinking about how to make users rationale agents in the algorithmic marketplace of ideas.

Media pluralism has been the primary way to ensure the positive and passive dimension of the right to freedom of expression. Together with media freedom, pluralism is a precondition for an open and dialectic debate in a democratic society. Even if scholars are not on the same page about media pluralism online,[227] and even how to measure its effect,[228] it cannot be neglected how, in the field of content, users are not independent agents but subject to private determinations without any instrument to understand how their expressions are moderated online. Once again, European constitutional (and even international) law can help within this framework. Precisely, it helps to move the perspective of freedom of expression in content moderation from a negative and active to a positive and passive dimension.

---

[227] Judit Bayer and Sergio Carrera, 'A Comparative Analysis of Media Freedom and Pluralism in the EU Member States' (2016) Study for the LIBE Committee <http://www.europarl.europa.eu/ RegData/etudes/STUD/2016/571376/IPOL _STU(2016)571376_EN.pdf> accessed 4 February 2020.; Peter Barron and Simon Morrison, 'Pluralism after scarcity: the benefits of digital technologies' LSE Media Policy Project blog (18 November 2014) <http://blogs.lse.ac.uk/mediapolicyproject/2014/ 11/18/pluralism-after-scarcity-the-benefits-of-digital-technologies/> accessed 27 January 2020.

[228] Kari Karppinen, 'The Limits of Empirical Indicators: Media Pluralism as an Essentially Contested Concept' in Peggy Valcke and others (eds), *Media Pluralism and Diversity: Concepts, Risks and Global Trends* 287 (Springer 2015).

In Europe, serious threats for fundamental rights can be considered as triggers of the States' positive obligation to regulate private activities to protect fundamental rights as underlined by the Strasbourg Court,[229] also in relation to the right to be informed.[230] As the Council of Europe underlined: 'As the ultimate guarantors of pluralism, States have a positive obligation to put in place an appropriate legislative and policy framework to that end. This implies adopting appropriate measures to ensure sufficient variety in the overall range of media types, bearing in mind differences in terms of their purposes, functions and geographical reach'.[231] As the UN special rapporteur on freedom of expression observed regarding the use of artificial intelligence technologies, 'human rights law imposes on States both negative obligations to refrain from implementing measures that interfere with the exercise of freedom of opinion and expression and positive obligations to promote the rights to freedom of opinion and expression and to protect their exercise'.[232]

The Strasbourg Court has not only underlined the democratic role of the media,[233] or the prohibition for States to interfere with freedom of expression. It went even further by recognising that Article 10 can lead to positive obligations.[234] For instance, in *Dink v Turkey*,[235] the court addressed a case concerning the protection of journalists expressions clarifying that States have a positive obligation 'to create […] a favourable environment for participation in public debate by all the persons concerned enabling them to express their opinions and ideas without fear, even if they run counter to those defended by the official authorities or by a significant part of public opinion, or even irritating or shocking to the latter'.[236] More recently, in *Khadija Ismayilova v Azerbaijan*,[237] the Strasbourg Court recognised that States are responsible to protecting investigative journalists. Besides, the protection of the right to freedom of expression under the Convention safeguards not only the right to inform but also the right to the receive information.[238] The Strasbourg Court has further clarified the characteristics of such a positive obligation in *Appleby and Others v UK*, precisely considering the nature of expression at stake and its role for public debates.[239]

With regard to the digital environment, the Strasbourg Court recognised the role of the Internet in 'enhancing the public's access to news and facilitating the dissemination of information in general',[240] underlining also that 'the internet has now become one of the principal means by

[229] See, for example, Von Hannover v Germany (2005) 40 EHRR 1; Verein gegen Tierfabriken Schweiz (VgT) v Switzerland (2001) 34 EHRR 159. See Lech Garlicki, 'Relations between Private Actors and the European Convention on Human Rights' in Andra Sajó and Renata Uitz (n 195), 129.
[230] See, e.g., Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v Austria (2013); Youth Initiative for Human Rights v Serbia (2013); Társaság a Szabadságjogokért v Hungary (2009); Sdruženi Jihočeské Matky v the Czech Republic (2006); Bladet Tromsø and Stensaas v Norway (1999).
[231] Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership (7 March 2018).
[232] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2018) <https://undocs.org/A/73/348> accessed 16 February 2020.
[233] See, e.g., Barthold v Germany (1985) 7 EHRR 383; Lingens v Austria (1986) 8 EHRR 407.
[234] See, e.g., Fuentes Bobo v Spain (2001) 31 EHRR 50; Özgür Gündem v Turkey (2001) 31 EHRR 49.
[235] Dink v Turkey (2010).
[236] Ibid, 137.
[237] Khadija Ismayilova v Azerbaijan (2019).
[238] Sunday Times v the United Kingdom (No. 1) (1979), 66.
[239] Appleby and Others v UK (2003).
[240] Cengiz and Others v Turkey (2015), 49, 52

which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest'.[241] Nonetheless, the court just addressed the problem of accessing information without scrutinising the criteria according to which information should be organised. Even if there is no consensus and how the introduction of artificial intelligence technologies in content moderation affects the right to receive information,[242] users still cannot access information about content moderation not only to understand the source and reliability of content they access but also remedy against discretionary harm coming from the block of accounts or the removal of content.

In the European framework, positive obligations in the field of content moderation would also derive from the need to ensure users a right to access remedies against the violations of their fundamental rights. According to Article 13 ECHR, 'everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity', along with the requirements of Article 1 on the obligation to respect human rights and Article 46 on the execution of judgments of the Strasbourg Court. This provision requires Contracting parties not just to protect the rights enshrined in the Convention but especially avoid that the protection of these rights is not frustrated by lack of domestic remedies. As observed by the Strasbourg Court, 'where an individual has an arguable claim to be the victim of a violation of the rights set forth in the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress'.[243] Similarly, Article 47 of the Charter provides even broader protection of this right being recognised by a general principle of EU law.[244]

Moving from the Convention to the Charter, it is worth recalling that Article 11 does not only protect the negative dimension of freedom of expression, but also the positive dimension of media pluralism when it states that '[t]he freedom and pluralism of the media shall be respected'.[245] To achieve this purpose, Member States are required to ensure not only to avoid interferences with the right to freedom of expression (i.e. negative dimension) but also diverse and plural access to content (i.e. positive dimension). In *Sky Österreich*,[246] the ECJ dealt with a case involving the protection of media pluralism relating to the financial conditions under which the provider is entitled to gain access to the satellite signal to make short news reports. In this case, the ECJ underlined the protection of the right to be informed or receive information guaranteed by Article 11 of the Charter as a limit to the freedom to conduct a business. In this case, by balancing the two fundamental rights in question, the ECJ gave priority to public access to information over contractual freedom. Nonetheless, once more, this case deals with access and not quality. It is also

[241] Ahmet Yıldırım v Turkey (2012), 54.
[242] Sarah Eskens and others, 'Challenged by News Personalisation: Five Perspectives on the Right to Receive Information (2017) 9(2) Journal of Media Law 259.
[243] Leander v Sweden (1987), 77.
[244] Case 222/84 Johnston v Chief Constable of the Royal Ulster Constabulary (1986) ECR 1651; Case 222/86 Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v Georges Heylens and others (1987) ECR 4097; Case C-97/91 Oleificio Borelli SpA v Commission of the European Communities (1992) ECR I-6313.
[245] Charter (n 51), Art 11(2).
[246] Case C-283/11 Sky Österreich GmbH v Österreichischer Rundfunk (2013).

not clear whether the EU framework could be influenced by the positive obligations of the Convention. It is true that the Charter provides a bridge between the two systems by stating that 'the meaning and scope of [Charter's] rights shall be the same as those laid down by the said Convention'.[247]

Despite different interpretations, as observed by Kuczerawy, 'the duty to protect the right to freedom of expression involves an obligation for governments to promote this right and to provide for an environment where it can be effectively exercised without being unduly curtailed'.[248] In the field of algorithmic technologies, the Council of Europe has underlined the importance of ensuring different safeguards like contestability and effective remedies in relation to public and private actors.[249] Precisely, States should ensure 'equal, accessible, affordable, independent and effective judicial and non-judicial procedures that guarantee an impartial review, in compliance with Articles 6, 13 and 14 of the Convention, of all claims of violations of Convention rights through the use of algorithmic systems, whether stemming from public or private sector actors'.[250]

Therefore, the potential regulation of content moderation would not just result from the need to balance other constitutional interests. Injecting democratic safeguards in the process of content moderation would aim to enhance the effective protection of the right to freedom of expression rather than undermining it. Besides, it is not only the right to freedom of expression but also the freedom to conduct business to be limited by the prohibition of abuse of rights.[251] In other words, the freedom of platforms to define the degree of protection of the right to freedom of expression online could not go so far to undermine of protection of the other constitutional rights.

The logic of moderation limits the transparency and accountability of online platforms, thus, marginalising users from understanding how content is processed in the digital environment. Since users cannot generally rely on horizontal and general rights vis-à-vis online platforms, this situation leaves these actors free to decide how to balance and enforce fundamental rights online without any public guarantee. Since the liberal approach to free speech (i.e. the free marketplace of ideas) has shown collateral effects in the digital environment, the protection of the negative side of this freedom is not enough to protect constitutional rights any longer. Therefore, in order to reduce the power of multinational private companies moderating content on a global scale, it is worth proposing a positive dimension of freedom of expression, triggering a new regulatory intervention towards the adoption of safeguards. In a way, this approach would fill the gap of something that should have been done in the last twenty years when recognising the power of online platforms to moderate speech without public guarantees.

At first glance, addressing this issue could lead to changing the liability system of online platforms to increase their degree of responsibility in online content moderation. Nevertheless, this kind of regulatory approach could undermine the economic freedoms of online platforms,

---

[247] Charter (n 51), Art 52(3).

[248] Aleksandra Kuczerawy, 'The Power of Positive Thinking. Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression' (2017) 3 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 182, 186-7.

[249] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (8 April 2020) <https://www.statewatch.org/media/documents/news/2020/apr/coe-recommendation-algorithms-automation-human-rights-4-20.pdf> accessed 1 October 2020.

[250] Ibid.

[251] Convention (n 52), Art 17; Charter (n 51), Art 54.

which would be overwhelmed by disproportionate obligations. Moreover, changing the safe harbour system would not solve the issue of transparency and accountability in online content moderation. Increasing legal pressure on social networks by introducing monitoring obligations would result in 'overly aggressive, unaccountable self-policing, leading to arbitrary and unnecessary restrictions on online behavior'.[252] This risk, known as collateral censorship, could have strong effects on democracy, thus, requiring regulators to avoid threatening online platforms for failing to correctly police content. [253] Due to the ability to govern their digital spaces through content moderation, governments find themselves stuck in cooperating with online platforms. Apart from the risks of surveillance, even the best-equipped public body for enforcement would be overwhelmed to handle all the content that platforms moderate thanks to their integrated systems and expertise. It is true that, in a perfect world, we would expect that decisions about rights and freedoms are covered by safeguards and guaranteed by independent public bodies. Nonetheless, reality shows that the fight against illegal content would be hard without online platforms. This does not mean renouncing to safeguards but recognise the limits of public enforcement in the digital environment. Therefore, the match is not between private and public enforcement but how to put together the two systems by injecting democratic safeguards in the relationship between public and private actors.

The aim of this new positive approach is not to make platforms liable for their conducts, but responsible for protecting democratic values through more transparent and users' driven procedures. A solution could consist of regulating diversity.[254] Some algorithms can be designed to increase diversity and operate ad adversarial to profiling. In other words, algorithms could also be a support to ensure pluralism and fight the process of targeting based on users' interaction and network (e.g. echo chambers), thus, reaching serendipity.[255] The European Commission's Code of Practice on Disinformation has encouraged platforms to conduct a process of dilution to tackle disinformation by improving the findability of trustworthy content.[256] This is would be a way to frame the role of algorithms not only as a risk but also as a support for democratic values where diversity becomes a policy goal in the information society.[257] In other words, such a new positive framework of freedom of expression would address the process of moderation without regulating content or changing platforms' immunities.

Therefore, at this time, the issue to solve is not just relating to the liability of online intermediaries but the injection of new safeguards.[258] Here, the proposal for a positive framework

---

[252] Milton Mueller, 'Hyper-Transparency and Social Control: Social Media as Magnets for Regulation' (2016) 39(9) Telecommunications Policy 804, 809.
[253] Jack M. Balkin, 'Free Speech and Hostile Environments' (1999) Columbia Law Review 2295.
[254] Maria Luisa Stasi, 'Ensuring Pluralism in Social Media Markets: Some Suggestions' (2020) EUI Working Paper RSCAS 2020/05 <https://cadmus.eui.eu/bitstream/handle/1814/65902/RSCAS_2020_05.pdf?sequence=1&isAllowed=y> accessed 15 June 2020.
[255] Judith Möller and other, 'Do not Blame it on the Algorithm: An Empirical Assessment of Multiple Recommender Systems and their Impact on Content Diversity' (2018) 21(7) Information, Communication & Society 959.
[256] Code of Practice on Online Disinformation (n 180).
[257] Brigit Stark and others, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse' Algorithm Watch (26 May 2020) <https://algorithmwatch.org/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf> accessed 7 June 2020.
[258] Aleksandra Kuczerawy, 'Safeguards for Freedom of Expression in the Era of Online Gatekeeping' (2018) 3 Auteurs & Media 292; Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a

of freedom of expression is focused on the proceduralisation of content moderation which would not affect platforms' immunity or the algorithmic structure. As the Council of Europe stressed, 'This positive obligation to ensure the exercise and enjoyment of rights and freedoms includes, due to the horizontal effects of human rights, the protection of individuals from actions of private parties by ensuring compliance with relevant legislative and regulatory frameworks. Moreover, due process guarantees are indispensable, and access to effective remedies should be facilitated vis-à-vis both States and intermediaries with respect to the services in question'.[259] Without regulating online content moderation, it is not possible to expect that platforms would turn their business interests driven by profit maximisation to a constitutional oriented approach. New procedural rules would allow users to rely on safeguards against potential violation of their fundamental rights resulting from discretionary decisions by platforms concerning online content while providing proportionate obligations in the field of content moderation.

Besides, this positive approach to freedom of expression could also advantage online platforms. A harmonised regulatory framework of content moderation would reduce the costs of compliance while enhancing legal certainty and their freedom to conduct business. The liability regime established by the e-Commerce Directive could be replaced a uniform system of rules and safeguards to increase harmonisation in the internal market. It should not be forgotten that the market is not made just of tech giants able to comply with any regulation. Therefore, the regulation of content moderation should provide a layered scope of application which takes into consideration small and medium-size businesses. Otherwise, the risk is to create a legal barrier in the market, fostering the power of some online platforms. A new set of rules on procedural transparency and accountability would reduce the challenges raised by regulatory fragmentation and legal uncertainty which platforms face when moderating content. Even the complementary introduction of a 'Good Samaritan' clause could increase legal certainty by breaking the distinction between active and passive providers and encourage platforms to take voluntary measures. Nonetheless, the solution of European digital constitutionalism would lead to increase transparency and accountability in the process of content moderation while maintaining the exception of liability of online platforms.

In order to understand the complexities resulting from the regulation of content moderation, the next subsections aim to provide a normative framework based on harmonised safeguards to increase the degree of transparency and accountability as well as avoiding discretionary interference with fundamental rights. The following analysis of users' safeguards is based on four general principles: ban of general monitoring obligation; transparency and accountability in content moderation; proportionality of the obligations; availability of human intervention. Precisely, according to the first principle, Member States should not oblige platforms to generally moderate online content like established by the e-Commerce Directive.[260] This ban is crucial to safeguard fundamental rights such as freedom to conduct business, privacy, data protection and,

Framework to Redress Predictive Privacy Harms' (2014) 55 Boston College Law Review 93; Danielle K Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1.

[259] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (2018).

[260] E-Commerce Directive (n 122), Art 15.

last but not least, freedom of expression.[261] Secondly, content moderation rules should be explained to users *ex ante* in a transparent and user-friendly way and ex-post when content is removed or blocked. The 'content moderation notice' should include the guidelines and criteria used by online platforms to moderate content and explain the company's internal process to ensure that decisions are as predictable as possible. The third principle aims to strike a fair balance between the rights of users and obligations of platforms. Although the lack of transparent and accountable procedures relegates users in a position of *subjectionis,* however, the enforcement of users' rights should not lead to a disproportionate limitation to the right and freedom of online platforms in performing their business, especially for protecting new or small platforms. The fourth principle is based on introducing the principle of human-in-the-loop in content moderation. The role of humans in this process could be an additional safeguard allowing users to rely on a human translation of the procedure subject to specific conditions.

Within this framework, the process of content moderation has been divided into three parts: notice system, decision-making and redress. First, the notice phase includes the ex-ante and ex-post information to disclose about moderation. Second, the decision-making phase concerns the reasons and effects of decisions such as content removal or blocking of accounts. Thirdly, the phase of redress regards the possibility for users to ask online platforms for a review of the first decision subject to specific conditions.

6.1 Notice System

The notice system is the first step of the process. It can be divided into ex-ante 'content notice' and ex-post 'user notice'. The former primarily concerns the information users should access about how content are organised and moderated by the platform while the latter focuses on the information concerning the process of hard moderation. The relevance of users' notice for content moderation has been already underlined as a sort of crowd-sourced censorship where users are an active part of the flagging system without being compensated for this activity.[262] Users are critical pieces of the content moderation puzzle since social media also rely on users to flag or, generally, report content.[263] On the opposite, in the phase of soft moderation, users have not instruments to influence how content is organised, precisely what is indexed, hidden or even filtered from their newsfeed or search results.

Despite its relevance, users' notice primarily concerns the phase of post-moderation. Nevertheless, as already underlined, moderation of content is also autonomously performed ex-ante by automated means, for instance, to recommend and organise content as well as to tackle extreme expression like terrorist videos when uploaded. Therefore, before focusing on removal or blocking of content, it is critical to outline a procedural framework according to which online platforms provide information to explain users the rules governing the organisation and processing of their online content. In other words, the content notice would foster transparency in

[261] See, for example, Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (2011); Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (2012).
[262] Eugene Morozov, *The Net Delusion* (Penguin Press 2012).
[263] Crawford and Gillespie (n 149).

content moderation by allowing users to understand not only how content is processed by online platforms, once they receive users' complaints, but also in the phase of pre-moderation.

Providing clear rules in the ex-ante face of the notice system aims to increase users' awareness of online content moderation. Precisely, this phase could involve the disclosure of the rules on which content moderation is performed to organise information. The content notice would increase legal certainty and predictability of removal decisions affecting fundamental rights. Precisely, online platforms could be required to publish their content moderation guidelines where they explain how the process is organised and the criteria used to moderate content such as definitions of infringing content and the criteria to moderate each type of content. Besides, the content notice would also consist of leaving users more freedom in self-determining the organisational criteria governing their content. What it lacks in the online public sphere is the possibility for users to select the criteria according to which information is organised. It is true that signing up on Facebook or Twitter is not mandatory, so users can decide through which sources they access news and information and shape their own community. However, the Internet also concerns social life through digital spaces. Some services, precisely social media, are increasingly the common standard for sharing expressions and ideas online. Without using Twitter or Instagram, some categories of users could experience a sort of marginalisation from the community which they feel to belong. Therefore, it is not enough to observe these services are fungible, but it is time to think about how to ensure pluralism within the online platforms' environment. The possibility for users to contribute to defining to which information they want to be exposed is critical to increase diversity and provide them more freedom to self-determine their news feed. Fostering autonomy and self-determination is a primary channel to ensure democratic debate, thus, avoiding that users become addicted to the content whose appearance is not casual but answer a precise business logic.

This process would also foster accountability of online platforms. The introduction of the content notice would not imply to regulate each options user should be able to access in content moderation but recognise at least minimum safeguards that should be prescribed by law to avoid that online platforms can freely choose which information deserves to be disclosed to users. In this way, governments, users and civil society organisations could access more information about the process of content moderation and scrutinise the behaviour of platforms when moderating content. Even if online platforms publish transparency reports and community guidelines, this is just a small piece of content moderation process. The logic of moderation leads online platforms to hiding information within the wall of the social media' castles, while a democratic society should pretend that powers are more accountable and transparent.

Once online platforms provide users with information to understand how content moderation is performed and the available remedies, users should also be aware of the procedures to submit complaints and informed about the ongoing process of moderation (i.e. user notice). Since user notice generally triggers the responsibility of online platforms to act promptly to remove the online content in question, this step plays a crucial role for both platforms and users. On the one hand, the former can understand when the obligation to remove specific content arises, on the other hand, the latter can know when the process of post-moderation has been initiated. It is worth underlining that users' notice does not trigger in any case the obligation of online platforms to remove content. In the case of the CDA, online platforms are not obliged to remove content unlike the process of 'notice and takedown' introduced by the DMCA, then, also adopted by the e-

Commerce Directive. According to this system, once the notice provider submits its complaint to online platforms, the process of online content review starts since users' notice makes platforms aware of the presence of alleged illegal content. Furthermore, users' notice is not the only way for triggering platforms obligation to remove content since their awareness can also derive from other sources, for example, from the news or other events of public interests.

When addressing users' notice, the first step consists of understanding who is the notice provider. First, it would be possible to distinguish between notice sent by public and private actors. When the notice is submitted following a judicial order or the decision of an independent administrative authority, online platforms would be obliged to remove content without having the possibility to assess whether the content is lawful or unlawful. Instead, the notification from the Government and its dependent authorities should not fall under this category to ensure that these public actors do not exploit this preferential notice system as a free way to overcome any accountability and censor online speech. In this case, judicial and independent administrative authorities could have access to a separate process for notification to speed up content review and recover the time spent to assess the lawfulness of specific online content.

The case is different where notice providers are private actors. In this case, the primary issue is to decide whether all users are on the same position or, instead, some notice providers enjoy a privileged status (i.e. trusted providers). This category would include special notice providers that can rely on privileged channels to signalling content considered illegal. For example, newspapers and publishers could be trusted flaggers for content involving defamation or disinformation. The same approach could be adopted for other notice providers such as collecting societies for copyright content. Nevertheless, since this choice would empower some entities in deciding about speech online, it would be necessary that the categories of trusted flaggers are provided and periodically reviewed by law or, at least, by independent competent authorities. In both cases, it should be observed that online platforms maintain discretion in deciding whether to remove or block specific content since the notice does not result from an order issued by the judiciary or independent administrative authorities. Therefore, it would be possible to divide notice providers into three categories: public authorities, trusted providers and users.

The second step consists of understanding according to which conditions the notice could be considered valid to trigger the process of online content review. Indeed, it cannot be excluded that the information provided for by the notice provider could be not adequate to process users' requests. Precisely, the notice could lack the URL to identify the content at stake or do not explain what the issue at stake is.[264] This issue is strictly linked with the form according to which notices are sent to online platforms. According to the current system, a notice can also be sent by mail to online platforms. This fragmentation could be mitigated by requiring the introduction of forms with mandatory information. However, since, even in this case, this discretion would empower platforms to select which information the users should insert, it would be necessary to rely on criteria provided by law or competent authorities.

The third step focuses on determining the flow of notice between three entities: the notice provider, content provider and online platform. Once the notice provider sends its notice to online platforms, the notice provider could receive at least other two notices before the decision. The first notice could consist of an automatic reply confirming that the request has been received and

[264] Case C-324/09 L'Oréal SA and Others v eBay International AG and Others (2011) ECR I-6011, 122.

how the platform will process it. The second notice could occur before the decision is implemented. This second contact would allow the notice provider to decide to add other information or withdraw its complaint.

Within this framework, the notice should also involve the content provider. In order to ensure transparency in this process, it would be appropriate that content providers are informed about the review process which could potentially lead to the removal or block of one of their content. This notice could occur once the platform starts its reviewing process after receiving the notice from the notice provider. In this case, the content provider would have the opportunity to submit its observations and proves to contest the notice. In this way, the possibility for content providers to object complaints on their content would inject in this phase the rights to a fair hearing, adversarial proceedings and equality of arms in the process of content moderation. It cannot be excluded that, in the above-mentioned cases, the notice could be limited to protect other interests such as confidentiality or the need to maintain secrecy in ongoing investigations. These exceptions should set by law to avoid that platforms raise several exceptions undermining, *de facto*, the notice system. Furthermore, in order to avoid any abuse of the notice system, it would be necessary to set mechanisms of compensation against users' misconducts such as compensation for the damage caused by submitting false notice or information. These mechanisms aim to avoid overwhelming platforms with fraudulent requests.

Once these steps are completed, and online platforms adopt their decisions, another notice should be sent both to the notice and content provider to inform them about the result of content moderation. The sum of these notice would increase the proceduralisation of content moderation allowing to build a more transparent and dialectic procedure before the phase of decision-making.

6.2 Decision-making

Once machines or human moderators process content, online platforms are called to decide whether to maintain or remove expressions. Since decision-making is the phase firmly affecting fundamental rights, additional safeguards should be welcomed. The point is not only whether users are in the position to generally understand the criteria online platforms implement to moderate content but also to rely on safeguards when platforms decide the sort of their expressions.

First, as already observed, online content moderation is basically performed by a mix of human and algorithmic systems. This system can be implemented to autonomously decide whether to shut down content or suggest potential infringing content to human moderators. Since automation plays a crucial role in moderating content, one of the primary questions concerns how to ensure that automated decisions can be foreseeable and transparent. It is no coincide whether transparency is at the core of the debate about algorithms.[265] The risks for fundamental rights and democracy are strictly linked to the lack of transparency about the functioning of automated

[265] See Daniel Neyland, 'Bearing Accountable Witness to the Ethical Algorithmic System' (2016) 41 Science, Technology & Human Values 50; Mariarosaria Taddeo, 'Modelling Trust in Artificial Agents, A First Step Toward the Analysis of E-Trust' (2010) 20 Minds and Machines 243; Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11 Ethics and Information Technology 105.

decision-making processes.[266] Ensuring transparency could be complicated for reasons relating to the protection of other interests such as trade secrets.[267] The issue can be explained due to the impossibility to predict the result of algorithms and reconstruct the elements which have led to a specific output due to the vast amount of data involved.[268]

This possibility is of particular concern for users when observing some pitfalls in algorithmic decision-making processes. In order to address these challenges, the algorithmic process can be divided into three phases: input, process and output. First, algorithmic input is made of data which, then, is processed to obtain an output. Therefore, the quality of data firmly affects the algorithmic output. Although the entire automated process could fit with the purposes of content reviewing, however, the way according to which online platforms have trained algorithms could lead to unforeseeable outputs. Concerning the process, it is necessary to distinguish between deterministic algorithms and systems based on machine learning. In the first case, since the procedure is based on pre-established steps, the prediction of a specific outcome could be possible. When, instead, machine learning is involved in content moderation, it could become complex to explain the process made to reach a specific output. Some algorithms can be considered 'black boxes' since their internal processes are incomprehensible to humans.[269] The aim of algorithms in content moderation is not to censor but to classify information according to specific clusters where content is considered 'lawful' or 'unlawful'. As a result, online content as input is transformed into predictions of the lawfulness of such information as output. This process is based on the system of trial and error where algorithms are trained based on the accuracy of their decision. This mechanism explains why some algorithms still lack that degree of accuracy to detect infringing content or take into consideration the general background. As a result, notwithstanding the output is the most relevant part for users, it is just a small part of the algorithmic jigsaw.

Moreover, despite the relevance of artificial intelligence in content moderation, the role of human moderators in the phase of decision-making cannot be neglected since moderators around the world usually take the last decision. Usually, moderators can rely on less than a minute to decide whether to remove certain content.[270] This strict time frame could be considered a fundamental clue to argue how human moderators cannot consistently comply with either a legal standard or any internal guidelines. Therefore, the process of content moderation is left in the

---

[266] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society 1; Christopher Kuner and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 6 International Data Privacy Law 167; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', in Jacques Bus and others (eds), *Digital Enlightenment Yearbook* (IOS Press 2012); Meg L. Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216.

[267] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).

[268] Joshua A. Kroll and others, 'Accountable Algorithms' (2016) 165 University of Pennsylvania Law Review 633; Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) 6(3) Ethics and Information Technology 175.

[269] Pasquale (n 152); Maayan Perel and Niva Elkin-Koren, 'Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement' (2017) 69 Florida Law Review 181.

[270] Olivia Solon, 'To Censor or Sanction Extreme Content? Either Way, Facebook Can't Win' The Guardian (23 May 2017) <https://www.theguardian.com/news/2017/may/24/facebook-struggles-with-mission-impossible-to-stop-online-extremism> accessed 25 July 2019.

hand of moderators' will. It is worth observing that this activity is far from the judicial environment where a court decides whether content is illegal. While a trial could last years to decide whether a statement is defamatory, moderators take this decision in a bunch of seconds. They do not only lack legal skills but also come from very different backgrounds since the activity of content moderation is often outsourced to third countries.[271] The same concern can be extended to their working conditions which do not allow to perform the activity of content moderation with due care.[272]

Furthermore, automated and human moderation usually fails to reach a degree of granularity that allows taking into consideration the different nuances between contexts around the world. While automated technologies tend to classify content in different clusters consistently, values and principles are local and influenced by cultural diversities. Even if automated content moderation can help online platforms to perform this activity, their set of values and principles cannot reflect the multiplicities of communities in the world with the result that some content can be penalised for expressing values different from those on which algorithms have been trained and programmed. Still, for example, Zuckerberg markets Facebook as a global community.[273] Although online platforms found their narrative on their role in establishing and promoting the values of an open and global community, it is worth wondering how it is possible to agree on common rules between communities which, in some cases, are also made up of two billion of people.[274] Similar considerations apply to human moderator dealing with content concerning event far not only geographically but also culturally and socially. Moderators usually decide in less than a minute which content should be removed, no matter whether a specific content comes from different situations or environments.[275] While the activity of content moderation is easier for some content such as child abuse or terrorism, hate speech and disinformation could challenge both human and machine moderators.

Notwithstanding decision-making processes are often complicated to unbox, they ultimately affect users' fundamental rights since possible decisions are just 'ignore' or 'delete'. Within this framework, the primary question concerns the degree of explanation users should have the right to access. In the field of data, this issue has been discussed within the framework of the GDPR as we will see in Chapter VI. Just to anticipate the point in question, scholars have recently focused on understanding whether the GDPR provides a legal ground for individuals to defend themselves from potentially harmful consequences of the implementation of algorithms, most notably by creating a 'right to explanation' in respect of automated decision-making processes.[276]

---

[271] Paul M. Barrett, 'Who Moderates the Social Media Giants? A Call to End Outsourcing' (2020) NYU Center for Business and Human Rights <https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5ed9854bf618c710cb55be98/1591313740497/NYU+Content+Moderation+Report_June+8+2020.pdf> accessed 9 October 2020; Adrian Chen 'The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed' Wired (23 October 2014) <https://www.wired.com/2014/10/content-moderation/> accessed 22 July 2019.
[272] Roberts (n 128).
[273] Zuckerberg (n 127).
[274] Douglas Rushkoff, *Throwing Rocks at the Google Bus* (Portfolio 2016).
[275] Roberts (n 128).
[276] See, e.g., Bryce Goodman and Set Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 AI Magazine 50; Andrew D. Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7 International Data Privacy Law 233.

The same challenges can be extended to the field of online content since decisions affecting users' rights could be completely automated. First, in the content notice, users should be able to access ex-ante explanations about the logic used by online platforms to moderate content. Second, although it would be burdensome, or even impossible, for online platforms to provide a full human motivation for any decision, users should receive at least information about the decision such as the result of the review, information about redress mechanisms, the location, timing and identification number of the moderator who has reviewed a specific content. More importantly, since any restriction of content constitutes an interference with freedom of expression, online platforms could provide *ex ante* a human rights assessment about the impact of their decision making and *ex post* provide a brief explanation of the reason for the removal indicating on which ground the content has been eliminated (prescribed by law), for which purpose (legitimate aim) and the criteria used (proportionality). Therefore, moderators should not limit their activity to a binary decision ('ignore' or 'delete') but insert even brief information about the removal.

Third, human moderation constitutes a crucial safeguard in the decision-making phase to fill the 'black boxes' gap. However, a general rule applying human intervention to all the situation could be a burden for online platforms. In this scenario, the right to rely on human intervention in online content moderation could be applied at users' request and based on the type algorithms used for content moderation. More specifically, in this case, it would be possible to apply a system of 'scale protection' where human intervention is increasingly required as long as algorithms are less deterministic or explainable. For example, where machine learning technologies are involved in content moderation, human intervention could apply by default. Moreover, human intervention could be limited when the decision is the result of a notice coming from public authorities or a trusted notice provider due to their peculiar role.

By implementing these safeguards concerning the phase of decision-making, users could access more information about the logic of a decision affecting its fundamental rights. Even more importantly, increasing users' awareness about the decision-making outcome is functional to introduce effective redress mechanisms.

6.3 Redress

The redress phase is the last and eventual step of content moderation. Once online platforms decide to remove or maintain content, users should be able to ask online platforms to review the previous decision subject to certain conditions. This right aims to provide users with a second chance, primarily when decisions are entirely the result of automated processes. The recognition of redress mechanisms is critical not only because of the inaccurate assessments that can derive from automated and human moderations. It would also make online platforms more responsible when deciding over content while increasing the degree of fairness and translate the right to appeal within content moderation. The effects of content removal go beyond the single user and produce (negative and positive) externalities for society at large.[277] Therefore, within this framework, the introduction of proportionate appeal mechanisms against platforms' decisions would increase the degree of transparency, accountability and fairness of content moderation.

[277] Yifat Nahmias and Maayan Perel, 'The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations' SSRN (24 April 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3565025> accessed 1 July 2020.

The need to recognise users a second chance would seem to be welcomed by Facebook which has launched its Oversight Board.[278] As Zuckerberg underlined, 'Facebook should not make so many important decisions about free expression and safety on our own'.[279] Even before the launch of this idea, in April 2018, Facebook started to show more interest in the appealing process as a consequence of its activity of content moderation.[280] By presenting the oversight board, Clegg underlined 'With our size comes a great deal of responsibility and while we have always taken advice from experts on how to best keep our platforms safe, until now, we have made the final decisions about what should be allowed on our platforms and what should be removed. And these decisions often are not easy to make – most judgments do not have obvious, or uncontroversial, outcomes and yet many of them have significant implications for free expression'.[281]

When focusing on redress mechanisms, it is possible to define four steps: modalities of access, reviewing process, motivation and remedies. The first point concerns the procedural rules, including the limits, which users should respect to access a system of redress of the platform's decision. The second concerns the substantive and procedural safeguards in the phase of review by the platform. The third focuses on the remedies which these mechanisms should provide.

Looking at modalities of access from a subjective perspective, firstly, it is necessary to focus on whether access to redress mechanism should be opened to content providers and notice providers both when online platforms remove online content and refuse to perform this activity. Recognising the right to redress mechanism just in one of the two cases could produce negative effects. On the one hand, when users can rely on this right only when online platforms refuse to remove or block content, this choice would encourage platforms to censor content to avoid the burden of redress mechanism with serious risk of collateral censorship. On the other hand, if access to redress mechanism would be possible only in case of removal or block, the gap between the two systems would favour content provider since notice provider could not rely on redress mechanism when their complaint has been rejected. This system would not involve public actors since they usually are those who notify online content. Instead, where public actors are content provider, they could be part of a redress mechanism.

Secondly, from an objective standpoint, it is also important to explain whether access to remedy is restricted to certain content. In case of decision taken to comply with the order of a public authority, redress mechanism should be restricted. When the decision comes from the private determination of the platform, in the case of content removal, every content should be subject to scrutiny since the decision has been taken by the platform which has autonomously decide to remove that content. When, instead, platforms decide to keep content online, in this case, appeal could be restricted to certain content. Since the involvement of a global community, users have different perceptions of legality online. Therefore, to avoid platforms being

[278] Klonick (n 162); Douek (n 162).
[279] Mark Zuckerberg, 'A Blueprint for Content Governance and Enforcement' Facebook (15 November 2018) <https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/?hc_location=ufi> accessed 24 June 2020.
[280] Monika Bickert, 'Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process, Facebook' (24 April 2018) <https://newsroom.fb.com/news/2018/04/comprehensive-community-standards> accessed 24 May 2020.
[281] Nick Clegg, 'Welcoming the Oversight Board' Facebook (6 May 2020) <https://about.fb.com/news/2020/05/welcoming-the-oversight-board/> accessed 1 July 2020.

overwhelmed, a filter could be applied based on international human rights standards to rely on a common framework to which States around the world are bound to respect.

Another condition for accessing redress mechanism could be based on the use of automated technologies. If, on the one hand, the first decision has been taken solely by automated technologies, the redress mechanism could always be accessible to allow users to rely on a human review. On the other hand, access to redress mechanism could be restricted when the decision has been taken only by humans or supported by automated systems. In this case, it is important to inform users about whether a human or machine has addressed the case in question. Furthermore, users should be able to rely on the possibility to obtain a second decision from a moderator based in the geographical region as close as possible to the user's location. In this way, moderation of content would be more granular and accurate according to the specific cultural and social context.

The clarity of motivation or the exhaustion of other remedies could be other two conditions limiting redress mechanism. It cannot be excluded that platforms would receive similar or almost identical complaints. In this case, if the cases are serial and the motivation of the first decision is provided explaining the reasons for the removal or maintenance of content, the access to redress mechanism could be subject to the discretion of the platform. In other words, a detailed motivation of the first decision could be considered a way to exempt platforms from implementing redress mechanisms and, at the same time, could encourage online platforms to provide more information about the first decision. Besides, establishing that users should exhaust potential other remedies before to ask a review of the first decision could provide a more balanced approach in the phase of redress.

The second point involves the review of the first decisions. The primary principle is the provision of human intervention. Redress mechanisms should not be based on machines' outcome but human assessment as a minimum standard. In this way, users should have the possibility to rely on humans to review previous decisions. Otherwise, an automated review of the first decision would make ineffective this right, especially when an automated system has been involved in the first decision. Therefore, it is important to think how the review board could be structured to ensure independency and what is the parameter that they should take into account to review a previous decision. In this case, if the decision would take by the same persons working for (or influenced by) online platforms, the review process could not be considered independent or impartial. Online platforms would not only be 'judge' but also part of the process since the review concerns its decision of moderation which is not guide by an independent sense of justice but maximisation of visibility and engagement. Besides, they would also be part of the process because the review decision concerns not only users' conducts but also the activity of moderation. In this case, by following the example of the Facebook Oversight Board, it could be possible to create an independent body to assess these cases. The Oversight Board is financially supported by trust fund which is independent from Facebook and cannot be revoked before 6 years.[282] The board will be made of up to 40 members with different skills, knowledge and expertise while identity is made public with varied and diversified skills, knowledge and expertise while respecting diversity.[283] Regarding the parameter, the review should not only rely on the terms of

[282] Oversight Board Bylaws (January 2020) <https://about.fb.com/wp-content/uploads/2020/01/Bylaws_v6.pdf> accessed 28 May 2020. Art 2, Section 1.3.1.

[283] Oversight Board Charter (September 2019) <https://about.fb.com/wp-content/uploads/2019/09/oversight_board_charter.pdf> accessed 28 May 2020. Art 1.

services of the online platform but also on the framework of the business sector responsibility to respect human rights. International human rights law should indeed be part of the review mechanism to provide a uniform term of review which is not subject just to the private determination of social media.

When focusing on motivation and remedies, it is worth observing that providing explanations for every decision could be potentially burdensome since online platforms should invest additional resources. From a procedural perspective, another point would be whether the review procedure should be oral or written and performed in a reasonable time. Due to the number of potential users' requests, the written procedure would be the most suitable for online content moderation. However, it cannot be excluded that, in some peculiar cases, platforms could provide a sort of alternative dispute resolution mechanism based on an oral hearing. In this case, without regulating the entire review process but to decrease the degree of discretion in the phase of redress, the law could establish at least some conditions, especially concerning the reasonable time frame which should be respected to review the first decision. In this case, since motivation would also contribute to setting up a coherent list of cases based on established precedents to limit further users' appeals, the explanation for removal or reinstatement should be required only to some platforms according to specific thresholds based, for example, on their global turnover. Review decisions should be available to users and published in online platforms' webpages.

The primary remedy would consist of dismissing the first decision. Whenever online platforms restrict content, they should ensure the possibility to reinstate content. If the user disagrees with the first decision and relies on the redress mechanism established by the platform, it is necessary that the content previously removed is still available if online platforms review their first decision. Therefore, the reinstatement of content should always be technically possible. Besides, it cannot be excluded a more detailed system where online platforms can review their decisions by restricting the removing or blocking to a geographical area or providing or banning users' profiles in case of repeated infringements. Even in this case, remedies should be provided by law to avoid that online platforms exercise quasi-public roles without any safeguard for users.

7. Expressions as Data

The relevance of constitutional law in the field of content moderation should be unveiled at this time. While constitutional provisions have been conceived as limits to the coercive power of the State, in the algorithmic society, an equally important and pernicious threat for freedom of expression comes from online platforms making decisions on expression based on their ethical, economic and self-regulatory framework. This situation leads European constitutional law to react to protect constitutional rights and liberties. This does not mean that we should neglect public actors' interferences with the right to freedom of expression but consider that limitations to the exercise of freedoms also come from private actors in the digital environment.

The current opacity of content moderation constitutes a challenge for democratic societies. If individuals cannot understand the reasons behind decisions involving their rights, primarily when automated decision-making systems are involved, the pillars of autonomy, transparency and accountability on which democracy is based are destined to fall. While, in the past, the liberal approach to free speech fitted with the purpose to safeguard democratic values in the digital environment, today, the emergence of new powers governing the flow of information would

require a shift from a negative dimension to a positive approach by regulating content moderation. The liberal approach transplanted in the Union from the western side of the Atlantic in the aftermath of the Internet has led online platforms to impose their authoritative regime on content based on a mix of technological and contractual instruments. The result of this situation has led users in a status of *subjectionis* where they find themselves forced to comply with standards of freedom of expression autonomously determined by online platforms. By referring to Balkin, there is the need for a 'new-school' of speech regulation which does not focus on old rules looking at speakers but to Internet infrastructure and actors involved.[284]

Within this framework, the Union has started to focus on introducing mechanisms of transparency and accountability in online content moderation. For example, the rights to obtain motivation or human intervention are still unripe but important steps towards a more democratic digital environment. These users' rights should not be considered only as instruments to improve transparency and accountability but also to limit the discretion of online platforms operating as private powers outside any constitutional boundary. Nevertheless, it is necessary to observe that Union efforts are not still enough to ensure a path towards the democratisation of the digital environment. Today, users can rely on certain rights only in the Union and just for specific content. This choice could lead to an axiological prevalence of some interests in online content moderation since users cannot generally rely on the same rights for all expression. Furthermore, the fragmentation of users' rights also affects the platforms' freedom to conduct business since it requires these actors to set different regimes of content moderation. However, this is not the only concern at stake. Notwithstanding the Union has introduced new safeguards in content moderation, online platforms still enjoy a broad margin of discretion to decide how to implement them. Regarding the notice system, it is not specified who could be considered trusted notice provider. Besides, the boundaries of motivation in content removal are not entirely clear. The same consideration applies for redress mechanism where the review of the platform's decision is not subject to any due process obligation.

Within this framework, the approach of the Union underlines the relevance of European constitutional law in reacting against new forms of powers raising transnational challenges and undermining democratic values. Like in the field of data protection as we will see in Chapter VI, the Union has started to pave the way towards the regulation of online platforms' activities with increasing convergence of safeguards in the field of data and content. In other words, the Union approach can be considered a first crucial step towards a new approach to content moderation where online platforms are required to operate as responsible actors in light of their gatekeeping role in the digital environment.

Still, the challenges to freedom of expression are not isolated. They are intimately intertwined with the protection of privacy and personal data. Content and data the two sides of the same coin of digital capitalism. This is evident even in content moderation where information shared by users often includes personal data which then are automatically processed for moderating expressions. The algorithmic society relies on the processing of (personal) data. Therefore, it is time to focus on the field of data to underline the role of European digital constitutionalism in protecting fundamental rights and democracy.

[284] Balkin (n 61).

Chapter VI

Digital Constitutionalism, Privacy and Data Protection

Summary: 1. Data in the Algorithmic Society. – 2. From the Right to Be Let Alone to the Rise of Automation. – 3. Data Protection in the Age of Big Data. – 4. Big Data and the GDPR. 4.1 The Notion of Personal Data. 4.2 General Principles. 4.3 Automated Decision-making Processes. – 5. A Digital Constitutional Interpretation. 5.1 Human Dignity. 5.2 Proportionality. 5.3 Due Process. – 6. Humans in the Algorithmic Society.

1. Data in the Algorithmic Society

The evolution of the algorithmic society has shed light on the relevance of data on daily life. Algorithms are becoming more pervasive, providing new opportunities of the private sector,[1] and even for the performance of public tasks.[2] The new possibilities raised by automated technologies has led to defining data as the raw materials of digital capitalism driving the fourth industrial revolution.[3] At the same time, these automated systems are increasingly surrounding individuals with technical systems influencing their decisions without the possibility to understand or control how the processing of their data affects their rights and freedoms.[4] Like in the case of freedom of expression, the implementation of algorithms challenges democratic systems due to the lack of transparency and accountability in decision-making affecting fundamental rights and freedoms.[5]

Algorithms have contributed to introducing new ways and models to process vast amounts of data. The organisation and dissemination of information in the digital environment, the profiling of consumers based on credit scores or new techniques in predictive law enforcement are only some examples of the answers which automated decision-making systems can provide and how such technologies can affect raise concerns not only from the perspective of individuals' rights and freedoms but also for democracy.[6] As Regan underlined, '[p]rivacy has value beyond its usefulness in helping the individual to maintain his or her dignity or develop personal relationships. Most privacy scholars emphasise the individual is better off if privacy exists. I maintain that the society is better off as well when privacy exists. I maintain that privacy serves not just

[1] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[2] Marion Oswald, 'Algorithm-Assisted Decision-making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power' (2018) 376 Philosophical Transaction Royal Society A.
[3] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).
[4] Carlo Casonato, 'Intelligenza artificiale e diritto costituzionale: prime considerazioni' (2019) Diritto Pubblico Comparato ed Europeo 101; Andrea Simoncini, 'L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà (2019) (1) in BioLaw Journal 63; Francesco Pizzetti (eds), *Intelligenza artificiale, protezione dei dati personali e regolazione* (Giappichelli 2018); Gabriele Della Morte, *Big data e protezione internazionale dei diritti umani. Regole e contenuti* (Editoriale Scientifica 2018).
[5] Paul Nemitz, 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) Royal Society Philosophical Transactions A.
[6] Brent D. Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679> accessed 27 August 2019.

individual interests but also common, public and collective purposes'.[7] Individuals tend to adapt their behaviours to a new societal form of surveillance or fear to express themselves, while new information asymmetries do not allow individuals to understand what is happening behind the scene.[8] The Orwell's dystopian scenario is not still the rule, but there is an increasing tendency in monitoring and classify human behaviours in every moment of daily lives.[9] From home application to biometric surveillance in public spaces, there are fewer private spaces where individuals can escape from the eyes of public and private actors. Nonetheless, this does not concern only the individual's private sphere but also the impossibility to scrutinise data collection and use.

The result is that digital technologies become an instrument for social control.[10] Individuals are increasingly transparent operating in a virtual world which is increasingly opaque. In 2010, Zuckerberg underlined 'The age of privacy is over'.[11] Under this perspective, algorithmic technologies are incompatible with data protection which is seen as an obsolete tool limiting unlimited datification of human life for business purposes. Put another way, we are experiencing a process where privacy becomes public while the processing of personal data opaque. These threats do not just involve the private sphere of rights and freedoms but also autonomy and awareness undermined by the lack of transparency and accountability. The case of Cambridge Analytica has been a paradigmatic example of the asymmetry of power in the data field, showing how the role of micro-targeting of voters for electoral purposes challenges fairness and transparency.[12]

When looking at the information society, the large exploitation of data from public and private actors put the protection of personal information under pressure. This why the reaction of digital constitutionalism does not just involve the right to freedom of expression. The new threats of the algorithmic society affect other two pillars on which liberty and democracy are based in the 'onlife' dimension, in particular the right to privacy and data protection.[13] The latter complements the protection of the former against the threats coming from profiling and mathematising human life. Privacy and data protection share a common objective, precisely protecting individuals' autonomy as a precondition to fully participate in social life. Therefore, the role of data protection in the information society is to provide safeguards for individuals to participate in the information society while maintaining control of their data and the manner in which it can be used. In this sense, data protection represents the 'positive' side of the rights to privacy against interference with the individuals' freedom to be let alone. Without rules governing the processing of personal data, individuals could not rely on guarantees protecting their privacy and autonomy against discretionary processing of personal information. Without accountability and transparency

[7] Priscilla M. Regan, *Legislating Privacy, Technology, Social Values and Public Policy* 321 (University of North Carolina Press 1995).
[8] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2018).
[9] George Orwell, *1984* (Penguin Books 2008).
[10] Stefano Rodotà, *Elaboratori elettronici e controllo sociale* (Il Mulino 1973).
[11] Marshall Kirkpatrick, 'Facebook's Zuckerberg Says the Age of Privacy is Over' The New York Times (10 January 2010) <https://www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html?source=post_page> accessed 5 October 2020.
[12] Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper Collins 2019).
[13] Luciano Floridi (ed.), *The Onlife Manifesto Being Human in a Hyperconnected Era* (Springer 2015).

safeguards, it is not possible to mitigate the asymmetry of power and mitigate the effects of automated decisions not only on individuals' fundamental rights but also democratic values.

In a world where machines increasingly make decisions on individuals' rights and freedoms based on opaque determinations, data protection would play a critical role. Data Protection regimes have been designed to deal with powers over information. The connection between algorithms and data is intimate. Even if not exclusively, the good performance of machine learning technologies is connected with data and, precisely, accuracy. Nonetheless, the processing of massive amount of data is not the only issue in the big data framework. There is also a process of data transformation able to produce new information and, therefore, value. Even if, at first glance, data can also be raw pieces of information, the same data can acquire huge value when analysed for a specific purpose and put together.[14]

Therefore, the constitutional values underpinning privacy and data protection can play a critical role in shaping the technological evolution of artificial intelligence. A liberal or protective frame characterising constitutional protection of these fundamental rights can make a difference in fostering or mitigating the rise of private powers in the field of data. It would be just enough to recall how the rise of European digital constitutionalism has led to a shift from an economic dimension in the protection of personal data as enshrined in the Data Protection Directive,[15] to the GDPR which dedicates its first Recitals to the importance of safeguarding privacy and data protection as fundamental rights in the European framework.[16] While, concerning content, the primary issue concerns the adoption of new rights and obligations to fill a democratic gap, the field of data is more mature. Nonetheless, even if the consolidation of the positive dimension of privacy in the right to data protection culminated with the adoption of the GDPR, European data protection law would require further steps forward to address the challenges of the algorithmic society. This process would not be based on introducing new safeguards but providing a constitutional oriented interpretation of the GDPR ensuring the protection of fundamental rights and democratic values while promoting innovation in the internal market.

Within this framework, this chapter aims to provide a constitutional interpretation of the relationship between artificial intelligence and data protection. Protecting privacy and data protection in the European framework does not consist of searching new rules to mitigate private powers but interpreting the GDPR under the lens of European digital constitutionalism. This chapter goes beyond the debate about the relationship between algorithms and data protection which have principally focused on specific sectors or issues like the right to explanation. Without merely focusing only on automated decision-making, this chapter underlines that, although the

[14] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 UC Davis Law Review 399.

[15] 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.

[16] 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. Francesco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo* (Giappichelli 2016); Francesco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016); Licia Califano, 'Principi e contenuti del Regolamento 2016/679/UE in materia di protezione dei dati personali' in Lucia Scaffardi (ed.), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale* 1 (Giappichelli 2018).

positive dimension of the right to data protection has been a critical step of digital constitutionalism, it is worth focusing on understanding the constitutional values underpinning the GDPR and its relationship with artificial intelligence. The centrality of data in the algorithmic society requires constitutional guidance to avoid that private interests prevail over fundamental rights and democratic values.

In order to achieve this purpose, the first part of this chapter focuses on the rise and consolidation of data protection as an answer to automation in the European framework. This part explains how and to what extent personal data have started to be protected in the aftermath of the information society. The second part addresses the rise of the big data environment and the constitutional challenges introduced by automated decision-making technologies. This part underlines that privacy and data protection are now facing another test in the algorithmic society. The third part focuses on the GDPR underlining the opportunities and challenges of European data protection law concerning artificial intelligence. This part aims to highlight to what extent the system of the GDPR can ensure the protection of the right to privacy and data protection in relation to artificial intelligence technologies. The fourth part underlines the values underpinning GDPR's safeguards to provide a constitutional interpretation of how the GDPR, as a mature expression of European digital constitutionalism, can mitigate the rise of unaccountable powers in the algorithmic society.

2. From the Right to Be Let Alone to the Rise of Automation

In the field of data, the role of digital constitutionalism in the algorithmic society could be observed by directly focusing on the GDPR's safeguard. At first glance, the relationship between data protection law and artificial intelligence could be examined looking at the structure and obligations of European data protection law. However, such an approach would provide just a limited picture of the underpinning values on which the right to data protection is based in Europe. Therefore, understanding which values characterise data protection is critical to provide a constitutional oriented interpretation of the GDPR. European data protection law is not just the result of regulatory but also historical reasons and constitutional values linked to the evolution of new technologies, precisely automated systems.

The European path towards the constitutional recognition of data protection as fundamental right started from the evolution of the concept of privacy in the US framework.[17] This right, namely 'the right to be let alone' by Warren and Brandeis at the end of the XIX century,[18] was conceived as negative liberty safeguarding of the individual's private life against potential external interferences.[19] Even in the European framework, privacy has been conceived as negative liberty. The Strasbourg Court underlined the right to privacy as the right to live far from publicity,[20] or away from unwarranted attention.[21] This right also extends to online anonymity,[22]

[17] Ugo Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto* (Giuffrè 2008); Antonio Baldassarre, *Privacy e Costituzione: l'esperienza statunitense* (Bulzoni Editore 1974).
[18] Samuel D. Warren and Louis D. Brandeis, 'The right to privacy*'* (1890) 4 Harvard Law Review 193.
[19] Daniel J. Solove, 'A Brief History of Information Privacy Law' (2006) Proskauer on Privacy; Alan Westin, *Privacy and Freedom* (Athenum 1967).
[20] X. v Iceland (1976) ECHR 7.
[21] Smirnova v Russia (2004) 39 EHRR 22.
[22] Delfi AS v Estonia (2015).

thus, enabling individuals to live peacefully in the online and offline environment. Nevertheless, the Strasbourg Court has not only underlined the right to privacy as a right to be let alone but also as a condition to development and fulfilment of personality, as well as personal autonomy and identity,[23] intimately connected with the right to human dignity in the European constitutional framework.

This focus on the individual is not by chance. When looking at the eastern side of the Atlantic, different underpinning values have guided the evolution and consolidation of the right to privacy and the rise to data protection.[24] As in the case of freedom of expression, the right to privacy in Europe is still a negative freedom but based on different constitutional premises. Already in Chapter I, we have underlined that liberty and dignity characterise respectively the western and the eastern sides of the Atlantic. The European experience has been traumatised by the second world war where even the right to privacy completely vanished.[25] The increasing amount of data collected for identifying people for creating government records based on data like ethnicity, political ideas and gender is a paradigmatic sample of how such a liberty was compressed. On the opposite, the US has not experienced such a violation of privacy and misuse of personal information, thus, encouraging a laissez-faire approach based on individual liberty. According to Whitman, Europe would be the dignity side of the Atlantic while the US would represent a model of privacy based on liberty.[26] The reality is more nuanced, but it cannot be neglected that the grounding values of the right to privacy across the Atlantic are different.[27] This is evident indeed when focusing on the evolution of the protection of personal data. In the US, the protection of privacy is not linked to the individual but to a sectorial approach and mosaic theory which looks at each individual as not relevant per se without the other mosaic tiles.[28] In other words, the personalistic characterisation of European data protection law cannot be found on the other side of Atlantic whose protection is centred on the sectorial and aggregated effects of certain processing of personal information, even if recently privacy and data protection are capturing more attention in the US framework.[29]

However, the historical reasons underpinning the constitutional differences across the Atlantic are not enough to explain the reasons triggering the positive evolution of the framework of data protection from the negative matrix of privacy. From a merely negative perspective (i.e. the right to be left alone), characterised by predominant liberal imprinting, the right to privacy in Europe has evolved towards a positive dimension consisting of the right to the protection of personal data.[30] This development can be mainly attributed to the increasing role of information to perform

[23] Reklos and Davourlis v Greece (2009) EMLR 290; Burghartz v Switzerland (1994) ECHR 22.
[24] Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).
[25] Elizabeth Harvey and others (eds), *Private Life and Privacy in Nazi Germany* (Cambridge University Press 2019).
[26] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) Yale Law Journal 1151.
[27] Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy' (2017) 106 Georgetown Law Journal 115.
[28] Orin S. Kerr, 'The Mosaic Theory of the Fourth Amendment' (2012) 111 Michigan Law Review 311.
[29] Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687.
[30] Sergio Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* (Cedam 2006).

public tasks and the evolution of new technologies. It firstly resulted from the increase in data usage and processing, primarily from the progress of the welfare state, the consolidation of new channels of communication (e.g. telephone), and automated processing techniques like databases.[31] In *Malone v The United Kingdom*, profiling citizens by the public authorities was highlighted as a dangerous trend threatening democratic society.[32] Computing (or information) technologies have introduced new possibilities for storage and organisation of data with lower costs. The advent of the Internet has not only lowered this cost but also increased the speed for transferring large sets of information and connect single nodes into a network for sharing data.[33] Thanks to the evolution of data management systems, the public and private sector was benefited from the new possibilities of the data-driven economy.

Nonetheless, this new framework has also introduced new risks related to the automated processing of personal data.[34] These developments affected the autonomy of individuals. The lack of control and safeguards against the massive collection and processing of data has enabled governmental authorities and private companies to take decisions without explaining which data have been used, for which purposes and duration. In 1983, the German federal constitutional court invalidated a federal law allowing the collection and sharing of census information between national and regional authorities.[35] The case involved the automated collection of personal data by public authorities for the performance of a public task. This decision, known as the *Volkszählungsurteil*, paved the way towards a right to 'informational self-determination' resulting from the constitutional interpretation of enshrining a general right to personality,[36] and the protection of human dignity.[37] This landmark decision highlighted the need to protect personal data from the interferences of automation and its connection with the autonomy and dignity of individuals. The court did not deny that data play a critical for the development of public policies and the pursue of public tasks in industrialised countries. At the same time, it shed light on the risks which the lack of individuals' awareness about the processing of personal data for public tasks in the field of tax or social security. This case has provided a first clue of the different characterisation of the right to privacy on the eastern side of the Atlantic and the role of a positive right to data protection aimed to protect the right to self-determination and human dignity.

It is not by chance that, in that period, some Member States had introduced data protection

---

[31] Jeffrey A. Meldman, 'Centralized Information Systems and the Legal Right to Privacy' (1969) 52 Marquette Law Review 335; Richard Ruggles, John de J. Pemberton Jr. and Arthur R. Miller, 'Computers, Data Banks, and Individual Privacy' (1968) 53 Minnesota Law Review 211; Arthur R. Miller, 'Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society' (1969) 67 Michigan Law Review 1089.

[32] Malone v the United Kingdom (1984) 7 EHRR 14.

[33] Helen Nissenbaum, 'Protecting Privacy in a Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

[34] Council of Europe, 'Convention no. 108/1981 - Explanatory Report', <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434>, visited 4 December 2018.

[35] BVerfG 15 December 1983, 1 BvR 209/83, *Volkszählung*.

[36] German Basic Law, Art 2(1).

[37] Ibid, Art. 1(1). See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review (2009).

regulation even before the advent of the Internet,[38] and anticipating the Data Protection Directive. Until 1995, at supranational level, data protection has been primarily addressed within the framework of the Council of Europe through the judicial interpretation of Article 8 of the Convention by the Strasbourg Court.[39] Together with the Convention, the Council of Europe has specifically focused on the challenges of automation for the right to privacy. In 1968, the Parliamentary Assembly of the Council of Europe proposed to establish a committee of experts to examine whether 'the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods'.[40] This acknowledgement of the role of new data processing techniques is also the reason for the adoption of the Convention No. 108 on the protection of individuals with regard to automatic processing of personal data adopted already in 1981.[41] This international instrument was the first to recognise the concerns relating to automated processing when either the Internet or artificial intelligence technologies have not still shown their ability to challenges the protection of personal data. Ensuring the protection of personal data taking account of the increasing flow across frontiers of personal data undergoing automatic processing was the first aim of this document which recently has been was modernised in 2018.[42] As a result, it is possible to underline the role played by automation in founding the constitutional basis for the new fundamental right of data protection whose aim is to protect 'every individual'.[43]

If, at that time, the Council of Europe could be considered the promoter of the constitutional dimension of personal data, this consideration can be extended only partially to the European Union. In this case, the Data Protection Directive regulated the processing of personal data only in 1995 and before the adoption of the Charter of Nice in 2000,[44] which recognised data protection as fundamental right,[45] albeit without any binding until the entry into force of the Lisbon Treaty in 2009.[46] As already seen in Chapter II, it would be enough to look at the Recitals of the Data Protection Directive highlighting the functional (and non-fundamental) nature of the protection of personal data for the consolidation and proper functioning of the single market and, consequently, as an instrument to guarantee the fundamental freedoms of the Union.[47] This

[38] See the *Datenschutzgesetz* adopted on 7 October 1970 in Germany; *Datalagen* adopted on 11 May 1973 in Sweden; Loi n. 78-17 6 January 1978 in France; Data Protection Act 1984 12 July 1984 in UK.
[39] European Convention on Human Rights (1950). See Leander v Sweden (1987) 9 EHRR 433; Amann v Switzerland (2000) 30 EHRR 843; S. and Marper v The United Kingdom (2008) 48 EHRR 50; M.M. v UK A no 24029 (2012) ECHR 1906. The ECtHR has justified such approach providing a definition of the Convention as a 'living instrument'. See, also, ECtHR, Mamatkulov and Askarov v Turkey (2005).
[40] Parliamentary Assembly of the Council of Europe, 'Recommendation 509 (1968) - Human Rights and Modern Scientific and Technological Developments', <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en>, visited 24 September 2019.
[41] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).
[42] Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.
[43] Ibid. According to Art 1: 'The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy'.
[44] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.
[45] Ibid, Art 8.
[46] Consolidated version of the Treaty on European Union (2012) OJ C 326/13, Art 6.
[47] Data Protection Directive (n 15). According Recital 3: 'Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons,

scenario based on the prevalence of the economic-functional dimension of the protection of personal data, the recognition of the binding nature of the Charter and the inclusion in the EU primary law have contributed to codify the constitutional dimension of the right to data protection in the Union.[48] This change of paradigm has led the ECJ to extend the boundaries of protection of these fundamental rights, thus, triggering a positive regulatory outcome with the adoption of the GDPR.[49]

In light of these considerations, the broad protection of personal data in Europe needs to be taken into consideration when addressing the relationship between artificial intelligence and personal data. It is not by chance that the right to privacy in Europe has been defined as the US First Amendment.[50] As observed by the ECJ, data protection needs to be ensured, primarily when automated processing is involved, thus, recognising a specific threat coming from automation and, *a fortiori*, on artificial intelligence technologies.[51] Data protection in the European framework constitutes a relatively new individual right developed as a response to the rise of the information society driven by new automated and digital technologies.[52] Unlike the case of freedom of expression, in this case, we have experienced the rise of the positive dimension of negative liberty to face the new challenges raised in the aftermath of the information society. The rise of data protection as an answer to the development of automated technologies would suggest that personal data would increasingly be protected to avoid the risks coming from the rise of the algorithmic society. If the right to privacy was enough to meet the interests of individuals' protection against public interferences, in the information society, the widespread processing of personal data through automated means and online sharing, has made no longer enough to protect only the negative dimension of this fundamental right.

Since data protection is a critical piece of the constitutional puzzle of the algorithmic society, it is worth focusing on the relationship between data protection law and artificial intelligence. The next section examines how the spread of big data analytics challenges the protection of personal data in the European framework.

3. Data Protection in the Age of Big Data

services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded'.

[48] Hielke Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU* (Springer 2016); Francesco Pizzetti, 'La privacy come diritto fondamentale al trattamento dei dati personali nel Trattato di Lisbona' in Paola Bilancia And Marialisa D'Amico (eds), *La nuova Europa dopo il Trattato di Lisbona* 83 (Giuffrè 2009).

[49] Giusella Finocchiaro, 'La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "Schrems"' (2015) (4-5) Diritto dell'informazione e dell'informatica 779; Oreste Pollicino and Marco Bassini, 'La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo' (2015) (4-5) Diritto dell'informazione e dell'informatica 741.

[50] Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25(2) European Law Journal 140.

[51] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (2014), 54 and 55 and Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015), 91. See, also, as regards Article 8 ECHR, S. and Marper v the United Kingdom (2008) 103, and M. K. v. France (2013), 35.

[52] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015). Gonzalez Fuster (n 24).

'Data is the new oil'.[53] This is one of the most common expression to describe the role of data in the information society where algorithmic processing contributes to the extraction and creation of value. Nonetheless, data do not exactly fit with this definition, precisely because their immateriality. Unlike oil, data can be reused multiple times, for different purposes and in non-rivalrous way without being consumed or losing their value. While oil is refined and consumed, the use of data is potentially perpetual like other information. The idea of data as oil however could be considered accurate when looking at the ability of data to generate value. Like oil for the industrial economy, the processing of a vast amount of data becomes a primary and endless source of values in the information society. As with other expressions in the field of new technologies, the term 'Big Data' has become a metaphor for the development of the information society.[54] In 2011, the term was used by the McKinsey Global Institute, which defined Big Data as data sets whose size exceeds a database's ability to acquire, store, manage and analyse data and information.[55]

At the beginning of this century, the Laney's three-dimensional model on data management based on Volume, Variety and Velocity already anticipated the premises of Big Data analytics.[56] These three Vs were developed in the context of e-commerce to generally describe the increase in the amount of data deriving from homogeneous and heterogeneous sources such as, for example, online accounts and sensors (i.e. Volume). Along with an exponential increase in the quantity of data, the sources have multiplied. If, on the one hand, the increase of volume constitutes one of the primary characteristics, on the other hand, the heterogeneity of the sources and types of data constitutes a fundamental element to fully understand the phenomenon of Big Data (i.e. Variety). In the past, the processing of data was characterised by structured data, namely information stored in databases organised according to rigid schemes. The development of new analytics techniques has allowed the exploitation of the so-called unstructured data or data that is not placed under any pattern or scheme.[57] The third element of growth is the rapid creation and sharing of data (i.e. Velocity). This model was then enriched by (at least) two other characteristics, namely Veracity and Value,[58] even if these elements reflect a different logic from the Laney's model based on incremental growth.

When we look at these characteristics in the context of the protection of privacy and personal data, the techniques used for processing purposes constitute a critical factor in the processing of personal data. It is no coincidence that Big Data analytics have been defined as 'the storage and analysis of large and or complex data sets using a series of techniques including, but not limited

[53] 'The World's Most Valuable Resource is no Longer Oil, but Data' The Economist (6 May 2017) < https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 26 February 2020.
[54] Cornelius Puschmann and Jean Burgess, 'Big Data, Big Questions. Metaphors of Big Data' (2014) 8 International Journal of Communication 1690.
[55] James Manyika and others, 'Big Data: The Next Frontier for Innovation, Competition, and Productivity', McKinsey Global Institute (2011) <https://www.mckinsey.com/business-functions/ mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation> accessed 3 March 2020.
[56] Doug Laney, '3D Data Management: Controlling Data Volume, Velocity and Variety' (2001) Application Delivery Strategies.
[57] Rob Kitchin and Tracey P Lauriault, 'Small Data, Data Infrastructures and Big Data' (2014) 80(4) GeoJournal 463.
[58] Chun-Wei Tsai and others, 'Big Data Analytics: A Survey' (2015) 2 Journal of Big Data 21.

to: NoSQL, Map Reduce and machine learning'.[59] The mix of these techniques is used for general value or to derive new information from apparently heterogeneous data. From traditional forms of data processing based on deterministic rules, Big Data analytics rely on new forms of processing using unstructured or semi-structured data such as multimedia content and social media accounts.[60] Content, blog posts, comments or accounts leave online traces revealing large parts of personal information. This also happens in a less transparent way, precisely when tracking the information left when surfing webpages or accessing online applications (e.g. cookies), or even systems to tracking users without any action (e.g. mobile applications).

Therefore, by looking at the combination between quantitative and qualitative data, it is possible to consider Big Data as a 'new generation of technologies and architectures, designed to economically separate value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and analysis'.[61] This definition can complement the idea of Boyd and Crawford who identified three criteria: technology, analysis and mythology.[62] By technology, they mean the mix of computing power and algorithmic methods capable of leading to the collection and analysis of large clusters of data. The analysis phase consists of identifying and predicting models that could have economic, social or legal effects. Mythology refers to the belief that new levels of forecast and knowledge can be obtained using these processing techniques. In light of these considerations, it is possible to define the phenomenon of Big Data as the collection and analysis of a large volume of structured and unstructured data through computational skills or algorithms to discover models and correlations that can lead to predictive analysis or automated decisions.

The relevance of the processing explains why the attention has been paid to the phase of analytics, namely the processing techniques (e.g. data mining) to define models or find correlations between structured and unstructured data sets.[63] The scope of this processing is different from the traditional search for information based on causal relationships. The implementation of algorithms in the phase of analytics has moved the focus from causality to probabilities and correlations. The vast amount of data does not allow to rely on traditional systems of processing, thus, encouraging to implement statistical methods. This shift from causality to probability is not neutral but raises concerns about the reliance on the outcome of these technologies.

This new framework has captured the European attention due to the challenges for protecting privacy and personal data. The WP29 underlined the growing expansion both in the availability

[59] John S. Ward and Adam Barker, 'Undefined By Data: A Survey of Big Data Definitions' ArXiv <http://arxiv.org/abs/1309.5821> accessed 6 February 2020.
[60] Richard Cumbley and Peter Church, 'Is Big Data Creepy?' (2013) 29 Computer Law and Security Review 601.
[61] Priyank Jain, Manasi Gyanchandani and Nilai Khare, 'Big Data Privacy: A Technological Perspective and Review' (2016) 3 Journal of Big Data.
[62] Danah Boyd and Kate Crawford, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2015) 15 Information Communication and Society 662.
[63] According to the European Union Agency for Cybersecurity (ENISA), Big Data analytics refers to 'the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours'. Giuseppe D'Acquisto and others, 'Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics', ENISA (December 2015) <https://www.enisa.europa.eu/publications/big-data-protection> accessed 3 March 2020.

and in the automated use of data analysed through automated systems. As underlined, 'Big Data can be used to identify more general trends and correlations but [...] big data may also pose significant risks for the protection of personal data and the right to privacy'.[64] The European Data Protection Supervisor has also intervened in this field by underlining how modern data collection and analytics techniques represent challenges for the protection of privacy and personal data.[65] Even the Council of Europe has adopted a definition that highlights the relevance of the new methods of data processing since, as regards the protection of privacy, the focal issues consists not just of the quantity and variety of the data processed but especially their analysis leading to predictive and decisional results.[66] In other words, the processing phase if the critical moment for the purposes of privacy and the protection of personal data since it does not only influence the collection of data but also the predictive and decision-making output. The phase of analytics can be considered, on the one hand, the step from which the value is extracted from the analysis of different categories of data. On the other hand, it is also the phase leading to the algorithmic output.

This focus on the challenges for individuals' rights and freedoms can be better understood if it is framed in a society where algorithms is increasingly implemented in decision-making and predictive models. Although these technologies have positive effects for the whole of society trusting the market to lead to new phase of growth, there are, on the other hand, consequences on fundamental rights and democratic values that cannot be overlooked. Although data constitute a crucial economic asset in the information society due to the value generated by its processing and marketing, at the same time, data can be closely linked to the individual identity and private sphere, thus, also involving the right to privacy. In other words, on the one hand, there is the interest to ensure that big data analytics keeps stimulating innovation of information society services by ensuring private economic initiative and the free flow of information. On the other hand, there is a need to avoid disproportionate interferences with the fundamental rights of individuals, primarily, privacy and data protection.[67]

At first glance, algorithms could be considered as neutral and independent system capable of producing models and answers useful for dealing with social changes and market dynamics. From a technical point of view, algorithms would be mathematical methods expressing results within a limited amount of space and time and in a defined formal language, transforming inputs, consisting of data, into outputs based on a specified calculation process. Nonetheless, from a social point of view, these technologies constitute decision-making process designed by

[64] Working Party Article 29, 'Opinion 03/2013 on Purpose Limitation' (April 2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 20 November 2019.

[65] According to the EDPS, Big Data refers to 'the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data". European Data Protection Supervisor, 'Opinion 7/2015, Meeting the challenges of Big Data' (November 2015) <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 4 March 2020.

[66] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01.

[67] Ian Lloyd, 'From Ugly Duckling to Swan. The Rise of Data Protection and its Limits' (2018) 34 Computer Law & Security Review 779; Charlotte Bagger Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 International Data Privacy Law 239.

programmers and developers. The human contribution in the development of these technologies leads to the translation of personal interests and values into algorithmic processes.[68] In other words, algorithms express results which, although determined by their code, constitute subjective determinations provided by automated systems. In this scenario, if from a technical point of view the algorithms are tools to extract value from the data, moving to the social perspective, these technologies constitute automated decision-making processes influencing the rights of individuals and society at large. The analysis of large amounts of data allows obtaining information about the behaviours, preferences, and lifestyles of data subjects.[69] The implementation of automated decision-making, especially based on machine-learning techniques, raises new challenges not only for privacy and data protection but also for the potential discriminatory and biased results coming from inferential analytics.[70]

If this scenario may not look less problematic at first glance, primarily, in the statistical or research field, however, the same processing acquires a different value when the categorisation of the individual in a group rather than in another one leads to a decision affecting individuals' rights.[71] Profiling and automated decisions are processes whose implicit scope is to divide groups of individuals into different categories based on common characteristics and make decisions based on belonging to a specific group.[72] Besides, profiling and automated decision-making does not only focus on the individual, but also clusters or groups based on common characteristics.[73] This automatic classification can lead to discrimination and serious effects on individuals' fundamental rights and freedoms.[74]

This is why algorithmic systems processing personal data are relevant for constitutional law. Big data analytics provide new opportunities for data analysis leading to insight into social, economic or political matters. At the same time, the probabilistic and statistic approach makes these outcomes problematic since correlation does not imply causation per se. If correlation overcome causation, constitutional democracies would deal with determinations whose degree of

---

[68] Philip A.E. Brey and Johnny Soraker, *Philosophy of Computing and Information Technology* (Elsevier 2009); Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press 1988).
[69] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1*;* Tal Zarsky*, '*Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375; Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2(2) Journal of Information Rights, Policy and Practice.
[70] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
[71] Brent Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303.
[72] Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "Right To Explanation"' (2016) 83 AI magazine 3.
[73] Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor and others (eds), *Group Privacy* (Springer 2017).
[74] Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 Journal of Big Data 12; Talia B. Gillis and Jann L. Spiess, 'Big Data and Discrimination' (2019) 86 The University of Chicago Law Review 459; Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6(2) Big Data & Society < https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805> accessed 12 October 2020.

error or inaccuracy is the natural result of the probabilistic logic. The European focus on the potential consequences of data analytics reveals the characteristics of the human matrix of the European protection of privacy and personal data once again. The processing of personal data is not only the engine of the fourth industrial revolution providing new opportunities for the internal market. Automated decision-making systems affect individuals' rights and freedoms, precisely the right to privacy and the protection of personal data as fundamental values of the European constitutional framework.

This challenge is increasingly relevant in the information society where the role of (personal) data plays a critical role in the public and private sector. As underlined by the GDPR, '(r)apid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their business goals. Natural persons increasingly make personal information available publicly and globally'.[75] Everything is transforming into digital data. At the beginning of this century, we have experienced the dematerialisation and digitisation of different products. Music, video and texts are nothing else that data. In the algorithmic society, the dematerialisation concerns the individual and its identity which is increasingly subject to process of datafication. Digital technologies have led personal information to be processed as data, thus, allowing to process also the most complex and intimate information concerning personal life.

Within this framework, data protection plays a critical role in the information society since the datafication of society make this fundamental right functional (or even necessary) to protect the right to privacy. Without ensuring that are processed according to safeguards based on transparency and accountability, it is not possible not only to protect the unlawful processing of personal data but also mitigate the interferences with the right to privacy. In other words, artificial intelligence technologies underline the critical role of data protection as a shield of individuals' self-determination and dignity against the new challenges raised by digital capitalism.[76] However, the role of data protection in the algorithmic society acquires a critical position not only to protects individuals' privacy but also as a safeguard for democratic values. The effective protection of privacy allows people to exercise their individuals' autonomy. In a democratic society, protecting privacy enables citizens to develop their believes, exchange freely opinions and express their identities. In order to promote autonomy and self-determination, it is critical that individuals can control their identity and how its personal information are processed.[77] One of the primary challenges for democracy would derive from regimes of public and private surveillance which, based on the processing of personal data, can lead to different profiling or targeting of users. This process cannot affect not only the right to privacy but also freedom of expression with clear effects on democratic values. This is why the liberal argument based on the lack of anything to hide fails to represent how people adapt their behaviours when they are observed or identifiable.[78]

---

[75] GDPR (n 16), Recital 6.

[76] Anne de Hing, 'Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation' (2018) 19(5) German Law Journal 1270.

[77] Charles Fried, 'Privacy: A Moral Analysis' (1968) 77 Yale Law Journal 475.

[78] Daniel Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press 2013).

Informational privacy is therefore critical for democracy,[79] but could not be enough without data protection law. Data protection indeed does not only protect individuals against surveillance but also foster transparency and accountability to mitigate asymmetries of powers threatening democratic values. The processing of vast amounts of data would lead to clear interferences with the possibility to understand how personal data are processed and according to which criteria. This is why data protection is a necessary piece of the democratic puzzle in the algorithmic society.[80] It allows citizens to make informed decisions (i.e. decisional privacy),[81] while protecting their private sphere. As a result, we cannot think a democratic digital society not only without privacy but also data protection. Within this framework, data protection plays a primary role to foster transparency and accountability against opaque processing, thus, promoting the right to privacy and self-determination as pillars for democracy. Nonetheless, as the next section shows, the relationship between European data protection law and artificial intelligence technologies is multifaceted.

4. Big Data and the GDPR

The adoption of the GDPR can be considered a milestone of European digital constitutionalism. Although, at first glance, this legal instrument aims to foster the protection of the right to privacy and personal data in the Union, the application of data protection rules to the algorithmic environment is far from being straightforward. The relationship between the GDPR and artificial intelligence is more nuanced than it can appear when looking at European data protection law. Artificial intelligence promises to provide new phases of growth for the internal market and foster fundamental freedoms while, at the same time, the massive automated processing of personal data leads to questioning the basic foundation of data protection law and challenges the protection of fundamental rights and freedoms.

This constitutional clash between risk and innovation implies that the implementation of artificial intelligence technologies does not only involve the responsibilities of data controllers or data subject's rights. These technologies profoundly challenge the pillars of European data protection law, including the notion of personal data and general principles. Even if, apparently, the GDPR has not been designed just to address the challenges raised by artificial intelligence technologies, there is an intimate connection between (constitutional) law and technology in this case due to the relevance of (personal) data in the artificial intelligence environment.[82]

Even before focusing on these constitutional challenges, it is worth underlining some regulatory choices which, even without directly involving artificial intelligence, affects the way the GDPR addresses the challenges of the algorithmic society. Precisely, the Union has decided to adopt a uniform framework of data protection by relying on regulation instead of directive like in 1995. This difference indicates a clear goal to overcome minimum harmonisation and increase

[79] Volker Boehme-Neßler, 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection' (2016) 6(3) International Data Privacy Law 222

[80] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth and others, *Reinventing Data Protection?* 45 (Springer 2009).

[81] Neil M. Richards, 'The Information Privacy Law Project' (2006) 94 Georgetown Law Journal 1087.

[82] Christopher Kuner and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 7(1) International Data Privacy Law 1.

the degree of coherence and cohesion in data protection law between Member States. If, at first glance, this political choice aims to ensure a uniform application of the European data protection law in the internal market, a more attentive legal focus shows how the GDPR provides several open clauses leaving Member States broad margins of discretion to implement provisions in national law. This has also been shown by the adoption of national laws by Member States to adapt their national legal framework concerning data protection to the GDPR's norms. A Regulation without open clauses would not have required such domestic efforts to adapt national law to the supranational framework of data protection. Such a choice is not neutral but produces consequences in terms of fragmentation and uncertainty concerning norms which are not ancillary but concerns critical points such as some of the legal basis for processing personal data,[83] including particular categories of data,[84] the exception in the field of freedom of expression,[85] or, even with regard to artificial intelligence, the right of individuals not to be subject to fully automated decisions.[86]

Despite the step forward in terms of harmonisation compared to the past, still the GDPR does not provide a monolith framework of protection. European data protection law still leaves Member States margins of discretion which can hinder the uniform protection against the challenges raised by the algorithmic society. In other words, the European fortress of personal data risks being fragmented in domestic connected castles which would challenge the ability of the GDPR to effectively safeguard fundamental rights and democracy across Member States. However, this risk of fragmentation does not exhaust these preliminary concerns. The GDPR requires companies to comply with material and organisational obligations requiring human and financial resources to avoid the imposition of high sanctions for failure to comply with data protection law.[87] For instance, the drafting of the Data Protection Impact Assessment or the appointment of the Data Protection Officer constitute two crucial requirements to respectively ensure an ex-ante risk assessment and monitor compliance, especially when the processing of data consisted of a systematic and extensive evaluation of personal aspects or monitoring of data subjects on a large scale.[88] If, on the one hand, these steps are not mandatory in any case, they could lead small business whose activities are based on the systemic evaluation of data subject to bear costs and face barrier to enter into the market of big tech giants.[89] In the lack of any exception for small and medium controllers, these safeguards could affect competition in the internal market. Besides, unlike transnational corporations, these entities would see in the GDPR not an opportunity to improve the protection of data as an asset of their business but as a threat from which it is necessary to escape. Such an approach could lead small and medium business to design their compliance without spending enough resources and time, thus, downgrading the level of protection for data subjects. Paradoxically, the structure of the GDPR would favour multinational

[83] GDPR (n 16). See Art 6.
[84] Ibid, Art 9.
[85] Ibid, Art 85.
[86] Ibid, Arts 22-23.
[87] Ibid, Art 83.
[88] Ibid, Arts 35(3)(a) and 37(1)(b).
[89] European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy', (March 2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 22 February 2020.

corporations hindering the development of start-ups and small tech businesses in the Union.[90] From a competition law perspective, this system would constitute a barrier to entry for new business and, since the processing of personal data involves all sectors, this system could favour only those entities owing the resources to comply with GDPR's obligations. Therefore, in the lack of any system encouraging new businesses to enter the market, the system of the GDPR could consolidate the economic power and, thus, the influence of some entities in the field of data.

Within this framework, the next subsections examine the relationship between artificial intelligence technologies and the GDPR, precisely by looking at the scope of personal data, the potential incompatibility with general principles, and challenges for data subjects coming from the implementation of automated decision-making technologies.

4.1 The Notion of Personal Data

The scope of application of the GDPR is firmly dependent on the notion of personal data. As already observed, such a personalistic approach characterises the European legal framework of protection in the field of data. In the information society, the economic value of Big Data comes from the processing of personal and non-personal data. Therefore, in order to trigger the machine of European data protection law, it is necessary to understand when there is a link between information and individuals defining data as 'personal'.

The GDPR applies only to the processing of 'personal data' as 'any information concerning an identified or identifiable natural person'.[91] While the notion of 'identified natural person' does not raise particular concerns for defining personal data, the notion of identifiability deserves more attention, especially when artificial intelligence technologies are involved. The GDPR provides a comprehensive approach concerning the identifiability of the data subject which can be identified by 'all means […] which the data controller or a third party can reasonably use to identify said natural person directly or indirectly'.[92] The assessment concerning the reasonableness of these means should be based on objective factors 'including the costs and the time required for identification, taking into account both the technologies available at the time of treatment and the technological developments'.[93]

Within this framework, the ECJ has extensively interpreted the notion of personal data extending its boundaries even to information apparently outside this definition. For instance, in *YS*,[94] the ECJ clarified that the data relating to an applicant for a residence permit contained in an administrative document, and the data in the legal analysis contained in that document, are personal data, while the analysis per se cannot be considered within this notion. Likewise, in

[90] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech' (2020) TILEC Discussion Paper No. 2020-012 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130> accessed 1 October 2020; Michal S. Gal and Oshrit Aviv, 'The Unintended Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349; Daniel L. Rubinfeld and Michal S. Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339.
[91] GDPR (n 16), Art. 4(1)(1).
[92] Ibid, Recital 26.
[93] Working Party Article 29, 'Opinion 4/2007 on the Concept of Personal Data' (June 2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en. pdf > accessed 26 February 2020.
[94] Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie (2014).

Digital Rights Ireland,[95] the ECJ recognised the relevance of metadata as personal data since they could make possible 'to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place'.[96] Therefore, the ECJ extended the notion of personal data considering even the risk of identification deriving from the processing of certain information.

The same approach was adopted in *Breyer*.[97] The dispute concerned the processing and storing of dynamic IP addresses of visitors to institutional websites by the German federal institutions to prevent cyber-attacks. The domestic court asked the ECJ whether the notion of personal data also included an IP address which an online media service provider stores if a third party (an access provider) has the additional knowledge required to identify the data subject. In *Scarlet*,[98] the ECJ had already found that static IP addresses should be considered personal data since they allow users to be identified. In this case, the attention is on dynamic IP addresses that cannot independently reveal the identity of a subject as they are provisional and assigned to each Internet connection and replaced in the event of other accesses. Therefore, the primary question focused on understanding whether the German administration, as the provider of the website, was in possession of additional information that would allow the identification of the user. The ECJ identified such means in the legal instruments allowing the service provider to contact, precisely in case of cyber-attacks, the competent authority, so that the latter takes the necessary steps to obtain this information from the former to initiate criminal proceedings. As a result, firstly, this case shows that, for the purpose of the notion of personal data, it is not necessary that information allow the identification of the data subject *per se*. Secondly, the information allowing identification could not be in the possession of a single entity.

The ECJ addressed another case enlarging the scope of the notion of personal data in *Novak*.[99] The case concerned the Irish personal data authority's refusal to guarantee access to the corrected copy of an examination test due to the fact that the information contained therein did not constitute personal data. After reiterating that the notion of personal data includes any information concerning an identified or identifiable natural person, the ECJ observed that, in order to answer the question raised by the national court, it is necessary to verify whether the written answers provided by the candidate during the examination and any notes by the examiner relating to them constitute information falling within the notion of personal data. The ECJ observed that the content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment as well as graphological information. The collection of these responses also has the function of assessing the candidate's professional skills and his suitability to exercise the profession in question. Finally, the use of such information, which translates into the success or failure of the candidate for the exam in question, can have an effect on the rights and interests of the same, as it can determine or influence, for example, his ability to access the desired profession or job. Likewise, with regard

[95] Cases C-293/12 and C-594/12 (n 51).
[96] Ibid, 26.
[97] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland (2016).
[98] Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (2011).
[99] Case C-434-16, Peter Nowak v Data Protection Commissioner (2017).

to the examiner's corrections, the content of these annotations reflects the examiner's opinion or evaluation on the candidate's individual performance during the examination, and, precisely, on his knowledge and skills in the field in question. Together with *Breyer*, this case shows an extensive approach to the notion of personal data with the result that it is not possible to foresee in any case when information should be considered 'personal' but it required the examination of the context through a case-by-case analysis.

In the field of artificial intelligence, this overall picture would lead to consider *a fortiori* how the dichotomy between personal and non-personal data looks less meaningful. Even if the processing of personal data through artificial intelligence technologies does not always involve personal data such as, for example, climatic and meteorological data, the potentiality of artificial intelligence technologies to find correlation through a mix of related and unrelated as well as personal and non-personal data, broadens the cases in which the scope of application of the GDPR cover processing of information which would not fall within the notion of personal data at first glance. For instance, big data analytics aims to identify correlations based on originally unrelated data.[100] It is the processing of different types of data that could lead to discovering or redefining data or information as personal.[101] It is no coincidence that some scholars have expressed their concerns about the impossibility to find information that cannot potentially be transformed into personal data.[102] In the information society, the economic value of Big Data comes from the processing of personal and non-personal data.

This consideration could be extended even to the process of anonymisation of personal data. The GDPR does not apply to anonymous data or information that does not refer to an identified or identifiable natural person or to personal data made sufficiently anonymous to prevent or disallow the identification of the data subject. Consequently, anonymised data would not fall within the scope of application of the GDPR. However, it could be easy to define the cases in which the anonymisation process is not reversible or apparently anonymous data are instead personal when mixed with other information. Therefore, there is no single definition of anonymous data, but this notion should be considered in the framework in which the data controller operates, taking into account 'all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.[103]

The primary criterion to assess whether data are anonymous come from a mix of factor and refers to the reasonable usability of the available means to reverse the process of anonymisation referring precisely to 'all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'.[104] According to Finck and Pallas, '[t]his difficulty is anchored in both technical and legal factors.

[100] GDPR (n 16), Recital 30. According to this Recital: 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them'.
[101] Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814.
[102] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.
[103] GDPR (n 16), Recital 26.
[104] Ibid.

From a technical perspective, the increasing availability of data points as well as the continuing sophistication of data analysis algorithms and performant hardware makes it easier to link datasets and infer personal information from ostensibly non-personal data. From a legal perspective, it is at present not obvious what the correct legal test is that should be applied to categorise data under the GDPR'.[105] Therefore, even data that would lead to the identification of personal information could be considered anonymous due to the absence of reasonable means to obtain from that information of a personal nature.

Nonetheless, as underlined by Stalla-Bourdillon and Knight, the approach to anonymisation would be idealistic and impractical.[106] This is because the phase of analytics plays a crucial role in the anonymisation of personal data. It is possible to observe how the quantity and quality of elements identifying the personal data influence the number of resources needed for anonymisation. There is a point where the resources available no longer allow the identification due to the number of data to be anonymised. The anonymisation process is effective when it can prevent anyone using reasonable means from obtaining personal data from anonymised data consisting of irreversible de-identification.[107] According to the WP29, 'the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, as permanent as erasure, i.e. making it impossible to process personal data'.[108] The concept of anonymous data still creates 'the illusion of a definitive and permanent contour that clearly delineates the scope of data protection laws'.[109] Anonymising data could not mean that we are not dealing with personal data any longer. Even when data controller makes almost impossible to identify the data subject, evidence shows that the risk of re-identification is concrete.[110] The WP29 has already underlined that the advance of new technologies makes anonymisation increasingly difficult to achieve.[111] Researches have shown the fallacies of anonymisation in different fields,[112] primarily when Big Data analytics is involved.[113]

Furthermore, even when focusing on pseudonymisation, we are still within the scope of application of the GDPR.[114] Pseudonymisation consists of 'the processing of personal data so that

[105] Michele Finck and Frank Pallas, 'They who Must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10(1) International Data Privacy Law 11, 11.
[106] Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data' (2017) 34 Wisconsin International Law Journal 284.
[107] Working Party Article 29, 'Opinion 05/2014 on Anonymisation Techniques' (2014), 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 19 June 2020.
[108] Ibid, 6.
[109] Khaled El Emam and Cecilia A´ lvarez, 'A Critical Appraisal of the Article Working Party Opinion 05/2014 on Data Anonymization Techniques' (2015) 5 International Data Privacy Law 73, 81–82.
[110] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105.
[111] Working Party Article 29 (n 107), 31.
[112] Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of Personally Identifiable Information' (2010) 53 Communications of the ACM 24, 26; Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069.
[113] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCL Law Review 1701.
[114] Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review 222.

personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organisational measures intended to ensure that such personal data is not attributed to an identified or identifiable natural person'.[115] The GDPR explicitly promote the use of this technique as a risk-management measure but not as an exception to its scope of application. Unlike anonymisation, the data controller can reverse pseudonymised data and this is why this information falls within the scope of personal data. Pseudonymisation consists just in the replacement of data with an equally univocal, but not immediately, intelligible information. Therefore, on the one hand, as long as data can be considered anonymous, this information can be processed freely by using big data analytics techniques, provided that, as already underlined, the processing does not lead to the identification of the data subject. On the other hand, in the case of pseudonymisation, the discipline of the GDPR applies and, as a result, the data controller is responsible for assessing the risks of this processing and relying on the appropriate legal basis. Furthermore, even if it cannot be excluded that, in some cases, pseudonymised data could be close to the notion of anonymity, they could fall under the processing of the GDPR allowing the data controller not to maintain, acquire, or process additional information if the purposes for which a controller processes personal data do not or do no longer require the identification of data subjects.[116]

Therefore, on the one hand, the GDPR would increase the protection of data subjects by extending the scope of the notion of personal data. The more the notion of personal data is broadly interpreted, the more the processing of data through artificial intelligence technologies falls under data protection law and, therefore, the processing of information through these technologies is subject to GDPR's safeguards. However, the impossibility to foresee when this technique could lead to the re-identification of data undermines legal certainty, thus, constituting a brake to the development of artificial intelligence technologies in the internal market.

4.2 General Principles

Artificial intelligence technologies do not just contribute to blurring the line between non-personal and personal data but also broadly challenge the general principles governing the GDPR. Once information falls within the category of personal data, the relationship between the GDPR and algorithmic processing is far from being exhausted. The challenges are not just about the scope of application of European data protection law but also its founding principles. It would be enough to look at the Charter underlining that 'data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[117] Together with other grounding values, the GDPR has introduced these principles representing the expression of the constitutional dimension of privacy and data protection as fundamental rights of the Union. The GDPR's general principles can indeed be considered the horizontal translation of constitutional values guiding data controllers when ensuring the

[115] GDRP (n 16), Art 2(5)
[116] Ibid, Art 11. In this case, the data controller is not required to comply with Articles 15–20 GDPR unless the data subject provides additional information enabling their identification for the purposes of exercising these rights.
[117] Charter (n 44), Art 8(2).

compliance with data protection rules and the protection of the data subject's rights. General principles play a crucial role in avoiding that processing of personal data leads to interferences with data subjects' fundamental rights. At the same time, they constitute axiological limits to the development of artificial intelligence technologies and the exercise of powers based on the discretionary processing of personal data.

Generally, the analysis of large quantities of data through opaque processing leading to outputs that are not always predictable are just some elements to consider when assessing the compatibility of big data analytics with the general principles of European data protection law. Such a multifaceted analysis of data for multiple purposes raises serious concerns, but not limited to, for the principles of lawfulness, fairness and transparency. These principles require natural persons to be made 'aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing'.[118] The obligations for the data controller to inform data subjects about the processing of their personal data,[119] or the legal basis for processing personal data are just two examples expressing (or implementing) the general principles.[120] As observed by Gutwirth and de Hert, whilst the right to privacy is an instrument of opacity for the protection of the individual, data protection plays the role of transparency tool.[121]

These principles are challenged by the algorithmic processing whose decision-making processes are often opaque.[122] These techniques do not always allow to explain data subjects the consequences of processing their personal data through such systems. For example, Big Data analytics often involves the re-use of data and leads to the creation of other information through inferences.[123] Therefore, it would not always be possible to predict from the beginning all the type of data processed and potential uses.[124] Therefore, the process of mandatory disclosure required by the GDPR would *de facto* fail before the characteristics of these technologies. It is no coincidence that Richard and King have defined this situation as a 'transparency paradox'.[125] On the one hand, big data analytics promises new levels of knowledge by defining models and predictions. On the other, the mechanisms by which these systems reach a new degree of knowledge are obscure. In other words, the price to access more knowledge is accepting a certain degree of data ignorance.

The information asymmetry between the data subject and data controller leads to questioning not only the principle of transparency but also of lawfulness and fairness. The lack of transparency

---

[118] GDPR (n 16), Recital 39.
[119] Ibid, Arts 14-15.
[120] Ibid, Arts 6, 9.
[121] Serge Gutwirth and Paul de Hert, 'Regulating Profiling in a Democratic Constitutional States' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* 271 (Springer 2008).
[122] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015); Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11(2) Ethics and Information Technology 105; Tal Zarsky, 'Transparent Predictions' (2013) 4 University of Illinois Law Review 1507.
[123] Sandra Wachter and Brent D. Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 494.
[124] Ira S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74.
[125] Neil M. Richards and Jonathan H. King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41.

in the processing would not always allow the data subject to express a valid consent.[126] Artificial intelligence technologies challenge how data subjects express their free and informed consent. In this situation where the data controller cannot explain the potential use of data transparently, the data subject is not aware of the risks when consenting to access products and services. Such information asymmetry is even more problematic when the data subject needs, for example, to access public services which are provided by a data controller or the data controller in a position of monopoly or oligopoly. According to the GDPR, the legal basis of consent should not be valid for processing personal data where there is a clear imbalance between the data subject and the data controller.[127]

Besides, the principle of lawfulness is undermined not only by the low level of transparency in the field of artificial intelligence but also by how information about the processing of personal data is shared with data subjects through privacy policies. This is not only relating to the use of long and complex explanations about the processing of personal data undermining *de facto* the possibility for data subjects to really understand how their personal data are used and for which purposes.[128] Another primary issue concerns the spread of daily lives applications (i.e. Internet of Things) collecting personal data in public and private places without the awareness of data subjects.[129] The strict rules to obtain consent and the burden of proof can prevent discretionary determinations over personal data but also encourage data controllers to rely on other legal bases beyond consent.[130]

This trend could be problematic for the principle of lawfulness also because the legal basis for the processing of personal data do not apply when the data controller process particular categories of data, namely 'those personal data that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical, or union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sexual life or sexual orientation of the person'.[131] As already observed, the analysis of a vast amount of data from heterogeneous datasets can lead to the discovering of new data (i.e. inferences) which could require a different legal basis to process them.[132] According to the WP29, '[m]ore often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern'.[133] In the algorithmic society, the rationale behind the distinction between 'ordinary' and 'particular' categories of data is completely nullified by the way in which the data are processed for at least two reasons. As already observed, first of all, Big Data analytics is based on a high volume of

[126] Alessandro Mantelero, 'The Future of Consumer Data Protection in the EU Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30(6) Computer Law & Security Review 643.
[127] GDPR (n 16), Recital 43.
[128] Aleecia M. Mcdonald and Lorrie F. Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 543.
[129] Carsten Maple, 'Security and Privacy in Internet of Things' (2017) 2 Journal of Cyber Policy 155; Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 85; Rolf H. Weber, 'Internet of Things – New Security and Privacy Challenges' (2010) 26(1) Computer Law & Security Review 23.
[130] GDPR (n 16), Recital 42.
[131] Ibid, Art 9.
[132] Wachter and Mittelstadt (n 123).
[133] Working Party Article 29 (n 64), 47.

structured and unstructured data, which usually do not rely on the distinction between categories of data. Secondly, data on health, race or sexual orientation can be obtained from the processing of unstructured data. For example, the contents of a social network account can reveal health or racial origin data that inevitably become part of the analysis process that leads to profiling or an automated decision. In other words, even non-particular categories of data can constitute a vehicle for the deduction of information of a particular nature. As noted by Zarsky, 'the rise of big data substantially undermines the logic and utility of applying a separate and expansive legal regime to special categories'.[134]

Such consideration also shows how artificial intelligence technologies challenge the principle of purpose limitation, precisely due to the multiple and unpredictable re-use of data.[135] It would not be by chance if the WP29 focused on the need to respect this principle in the field of Big Data by ensuring that the purposes for which the data is processed can be known or foreseen by the data subjects.[136] In order to comply with the principle of purpose limitation, it is necessary to inform the data subject of the processing whose purposes differ from the initial ones at the time of data collection and analysis. Therefore, the aim of this principle is to protect data subjects against the unforeseeable extension of processing purposes. The general use of Big Data analytics implies that data is not just held and used by a certain and predetermined number of third parties for a specific purpose. On the contrary, as observed by Mittelstadt, data 'travels with the person between systems and affects future opportunities and treatment at the hands of others'.[137]

Besides, the relevance of the principle of purpose limitation deserves to be examined not only by looking at the protection of data subjects' rights but also the effects such principle can produce on the internal market. It could constitute a barrier to the development of monopolies and dominant situations in the context of data analysis by limiting the possibility for data controllers to use data for any contingent purpose. Nevertheless, as Hildebrandt observed, a narrow interpretation of this principle could limit the potentialities of analytics which, usually, rely on creating models and previsions based on unrelated data and purposes.[138] The principle of purpose limitation can indeed constitute a barrier to data-driven innovation, especially for data sharing. However, what is defined as 'purpose limitation' could be more precisely described as 'non-incompatibility'.[139] Since it is not possible in some cases to foresee all the potential uses, the principle of purpose limitation would apply only in relation to that processing which is incompatible with those disclosed to the data subject.

Nonetheless, the challenges to the principles of transparency, lawfulness and fairness do not exhaust the concerns about the relationship between artificial intelligence and the GDPR's general

---

[134] Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 1014.
[135] Nikolaus Forgó and others, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales and others (eds), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation* 17 (Springer 2017).
[136] Working Party Article 29, 'Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of their Personal Data in the EU' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf> accessed 24 February 2020.
[137] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30(4) Philosophy and Technology 475, 482.
[138] Mireille Hildebrandt, 'Slaves to Big Data. Or Are We?' (2013) 17 IDP Revista de Internet Derecho y Política 7.
[139] Working Party Article 29 (n 64).

principles. The collection and analysis of vast amounts of data can affect the principle of data minimisation. Bygrave has described this principle as an instrument to ensure proportionality and necessity without exceeding the quantity of data to be processed.[140] Unlike the processing of data through analogical means, new automated processing techniques allow extracting value even from apparently unrelated data. This feature has been facilitated by the possibility of storing and analysing increasing amounts of data according to the so-called 'N = all' model according to which the collection and analysis of information are not based just on relevant data but on the whole.[141] The processing and accumulation of vast amounts of data also threaten the principles of integrity and confidentiality due to the increasing risks in handling large volumes of information to be managed.[142] The more data are processed and stored, the more will be the risk to face serious data breaches. Likewise, the trend towards data accumulation also could clash with the principle of data retention and security.[143] Dealing with large amounts of data processed for multiple purposes could make retention policies complex to implement and security measures subject to increasing layers of risks for the amount of data involved.

Even more importantly, the principle of accuracy is always involved because the result of automated decision-making is strongly influenced by the quality of data. Data mining techniques rely on various sources such as social media and other third-party sources that are known for not always being accurate. The pluralism of data sources increases the risk of dealing with inaccurate data.[144] This problem does not only occur *ex ante* when collecting and analysing data but also *ex post* due to the distorted effects that inaccurate data can have on the outputs.[145] According to Tene and Polonetsky, 'in a big data world, what calls for scrutiny is often the accuracy of the raw data but rather the accuracy of the inferences drawn from the data'.[146]

All these principles should be read in light of the principle of data controller's accountability, which is the ground of the GDPR's risk-based approach.[147] The data controller should be able to prove the compliance with general principles. The meaning of the principle of accountability can be better understood when focusing on the dynamic definition of the controller's responsibility based on the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[148] On this basis, the data controller is required to implement appropriate technical and organisational measures to guarantee, and be able to demonstrate, that the processing is carried out in accordance with the GDPR and, especially, its principles. According to the principle of privacy by design and by default,[149] the data controller is required to set adequate technical and organisational measures, such as pseudonymisation, to implement the principles of data protection effectively and to provide the necessary guarantees by design and ensure that, by default, only the personal data

[140] Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Wolter Kluwer 2002).
[141] Hildebrandt (n 138).
[142] GDPR (n 16), Art 4(f).
[143] Ibid, Arts 5(1)(e), 5(1)(f).
[144] Boyd and Crawford (n 62).
[145] Ibid, 662
[146] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 239.
[147] Ibid, Art 5(2).
[148] Ibid, Art 24.
[149] GDPR (n 16), Art 25.

necessary for each specific purpose are processed. For example, as far the principles of transparency or purpose limitation are concerned, data processing should allow the data subject to be aware of the modality of processing even when artificial intelligence technologies are involved, thus, requiring these technologies to take into consideration the requirement established by the GDPR. In other words, these principles would require data controllers to ensure ex-ante that the implementation of artificial intelligence technologies in the processing of personal data complies with the general principles of European data protection law. It is not always possible to ensure compliance with general principles when data controllers rely on artificial intelligence technologies to process personal data. In other words, the principle of accountability is the concrete expression of the challenges between algorithmic technologies and the general principles of European data protection law.

These considerations could be enough to explain the clash between artificial intelligence and European data protection law. Nevertheless, the implementation of automated decision-making technologies for processing personal data are also relevant to the protection of data subjects' rights, precisely when they lead to legal effects on their rights and freedoms.

4.3 Automated Decision-making Processes

One of the primary constitutional challenges for data protection in the age of artificial intelligence consists exactly of dealing with the lack of transparency and accountability in automated decision-making processes and their effects on individuals' fundamental rights and freedoms as well as democratic values. As already stressed, the involvement of algorithmic processing for purposes of profiling and automated decision-making challenges privacy and data protection.[150]

Automated decision-making could be defined as the process of taking decisions without human intervention. According to the GDPR, this process would consist of a decision based solely on automated processing.[151] Usually, these processes involve the use of artificial intelligence technologies. These techniques can indeed lead to binding decisions also depriving individuals of legal rights like accessing credit.[152] It is in this case that the GDPR aims to introduce safeguards to protect individuals against the discretionary use of personal data for purposes of automated decision-making. In order to empower data subjects to maintain control over their data and mitigate the asymmetry between the data controller and subject, the GDPR provides the so-called data subjects' rights.[153]

According to the GDPR, profiling consists of 'any form of automated processing of personal data consisting in the use of such personal data to evaluate certain personal aspects relating to a natural person, precisely, to analyse or foresee aspects concerning professional performance, the situation economic, personal health, preferences, interests, reliability, behaviour, location or movements'.[154] Against such processing, the data subject has the right to object at any time, for

[150] Bart W. Schermer, 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27(1) Computer Law & Security Review 45.
[151] GDPR (n 16), Art 22.
[152] Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41 Science, Technology, & Human Values 118.
[153] GDPR (n 16), Arts 15-22.
[154] Ibid, Art 4(4).

reasons connected with his particular situation. However, this right is not absolute. It can be exercised only when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,[155] or for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, primarily where the data subject is a child.[156] Therefore, the scope of such right is narrow and it cannot find a legal basis when profiling occurs based on the consent or the data subject or any other legal basis provided for by the GDPR.

Once the right to object has been exercised, the data controller cannot process personal data unless it demonstrates the existence of legitimate reasons prevailing over the interests, rights and freedoms of the interested party or to ascertain, exercise or defend a right in court. Furthermore, if personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data for these purposes, including profiling. In both cases, the data controller is explicitly required to present this information clearly and separately from any other information at the time of the first communication with the data subject.

This right empowers users to complain about the processing of its data when it is made by a public authority or it is the result of the choice of data controllers to rely on the legitimate interests as a legal basis of the processing, which, in any case, needs to balance the interest of the controller with the fundamental rights of the data subject. In this case, the right to object would allow users to intervene in this balancing which, otherwise, would be left in the hands of data controllers. In this case, the right to object protects data subjects against profiling by artificial intelligence technologies even if this right applies only based on these conditions.

Together with this safeguard, under the GDPR, individuals can rely on their right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern him or her, or that significantly affects his or her person.[157] The WP29 has clarified that the reference to the expression 'right' not to be subject to a decision based exclusively on automated processing does not imply that this guarantee only applies when the subject invokes this right, since 'individuals are automatically protected from the potential effects this type of processing may have'.[158] As pointed out by Mendoza and Bygrave, it is more appropriate to think this right as a prohibition rather than a right.[159] In this context, the principle of transparency would require the data controller to provide information to the data subject 'on the logic used, as well as the importance and the expected consequences of this treatment for the

[155] Ibid, Art 6(1)(e).
[156] Ibid, Art 6(1)(f).
[157] Stephan Dreyer and Wolfgang Schulz, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole' (2019) Bertelsmann Stiftung <https://www.bertelsmann-stiftung.de/doi/10.11586/2018018> accessed 12 March 2020; Isak Mendoza and Lee A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiani Synodinou and other (eds), EU *Internet Law: Regulation and Enforcement* 77 (Springer 2017).
[158] Working Party Article 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2018), 20 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 6 October 2020.
[159] Mendoza and Bygrave (n 157).

data subject', regardless of whether the data is collected by the data subject,[160] in line with the spirit of the GDPR which requires a high level of transparency in the processing of personal data.

By arguing *a contrario*, the lack of such a right would produce negative effects not only for individuals but also for democratic values since it would leave data controllers to fully rely on artificial intelligence technologies to make decisions affecting the right of data subjects without providing any safeguard like transparency and accountability for these outcomes. The lack of this safeguard is particularly evident by looking, for instance, at the framework of content moderation as examined in Chapter V. This freedom can be considered as the positive translation of constitutional rights within the legal regimes of data protection and, therefore, it applies to private actors without the need to rely on the horizontal application of fundamental rights. In this sense, the right not to be subject solely to automated decision-making processes increases the possibility for individuals to receive information about the automated decisions involving them and, therefore, foster the level of transparency and accountability.

Therefore, even if it is clear the relevance of this right within the framework of the GDPR, the question would be about the degree of transparency which the data controller should ensure. According to the GDPR, the data controller should provide meaningful information about the logic involved in the decision-making process.[161] In order to ensure transparency and fairness, it should take into account the circumstances and context of the processing, implementing appropriate mathematical or statistical procedures for the profiling, technical and organisational measures appropriate to minimise errors and inaccuracies, as well as safe procedures for personal data to prevent, *inter alia*, discriminatory effects.[162]

The right not to be subject solely on automated decision-making has triggered a debate among scholars, on whether the GDPR provides an effective legal basis for data subjects to avoid potentially harmful consequences deriving from the implementation of algorithms, most notably by relying on a 'right to explanation' in respect of automated decision-making processes.[163] Some of them argue that the GDPR introduce this right.[164] Other underlines that this right fosters qualified transparency over algorithmic decision-making,[165] deny the existence of such a right,[166] or doubt that the GDPR provisions provide a concrete remedy to algorithmic decision-making processes.[167]

It is not by chance that transparency is one of the most debated issues when focusing on

[160] GDPR (n 16), Arts 13(2)(f), Art 14(2)(g), Art 15(1)(h).
[161] Ibid, Recital 71.
[162] Ibid.
[163] See Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-making and a "Right to Explanation"' (2016) 38(3) AI Magazine 50.
[164] Mendoza and Bygrave (n 157); Andrew D. Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233. Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143.
[165] Margot E. Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkley Technology Law Journal 189.
[166] Sandra Wachter and others, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.
[167] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.

algorithmic technologies.[168] The challenges for individuals are intimately, even not exclusively, connected with the impossibility to ensure transparent outcomes of automated decision-making processes.[169] Despite the critics about the process of mandatory disclosure,[170] these obligations constitute an essential instrument to mitigate the asymmetries between data subjects and data controllers. The GDPR aims to increase data subjects' empowerment, thus, mitigating the technical opacity of automated decision-making.[171] The data controller should not only disclose the data used and the purposes of the processing, but it has also the duty to inform the data subjects about the use of automated decision-making and explain the logic of this process. These safeguards constitute a shield against potential predetermined and discretionary decisions against which the data subject would not have any remedy.

A further guarantee for data subjects against automated decision-making is provided by the limitation to the processing of particular categories of data provided for by the GDPR, without prejudice to the cases of explicit consent of the data subject and if the processing is necessary for reasons of significant public interest on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject.[172] We have seen how, in the field of big data analytics, profiling aims to create clusters of individuals based on their characteristics. Often, processing telephone numbers or name and surname would not be enough to develop predictive model since profiling focuses on the individuals' characteristics which constitute particular categories of data like health information, political ideas or even biometric data. Even in these cases, adequate measures have to be in force to protect the rights, freedoms and legitimate interests of the data subject.

Nevertheless, this data subjects' right is not absolute. The notion of 'legal or similarly significant effects' limit the general applicability of this data subjects' right.[173] The WP29 has also specified that this freedom applies just in cases of 'serious impactful effects' and when the automated decision could 'significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals'.[174] For example, this provision would apply when the data subject is applicant for a credit card as well as access to education or health services.

Moreover, several exceptions limit the scope of data protection safeguards. Unlike in the case of the notion of personal data and general principles, the GDPR provides a clearer set of exceptions to the application of this data subjects' right against automated decision-making processes. This liberty does not apply when the automated decision is necessary for the conclusion

[168] See, e.g., Daniel Neyland, 'Bearing Accountable Witness to the Ethical Algorithmic System' (2016) 41 Science, Technology & Human Values 50; Mariarosaria Taddeo, 'Modelling Trust in Artificial Agents, a First Step Toward the Analysis of E-Trust' (2010) 20 Minds and Machines 243.
[169] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus and others (eds), *Digital Enlightenment Yearbook* (IOS Press 2012).
[170] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250.
[171] Veale and Edwards (n 167).
[172] GDPR (n 16), Arts 9(2)(a), 9(2)(g).
[173] Ibid.
[174] Ibid.

or execution of a contract between the interested party and a data controller as well as when it is authorised by Union or Member State law to which the data controller is subject, which also specifies appropriate measures to protect the rights, freedoms and legitimate interests of the data subject. Moreover, it does not apply even when the processing is based on the explicit consent of the data subject. However, when the processing is based on a contract or the explicit consent of the data subject, the data controller is required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In this case, this prohibition turns into a right when the GDPR recognises that the data subject should at least have the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. This data subject's safeguard cannot lead to 'fabricating human involvement' since the human involvement and oversight should be meaningful.[175]

Furthermore, the data controller may limit the boundary of the right to explanation by invoking its interest to protect the trade secrets and intellectual property rights,[176] or, more generally, its freedom of economic initiative that would be frustrated by complying with transparency obligations requiring unreasonable resources.[177] For instance, when the techniques of data analysis through machine learning are involved, it is possible to highlight the so-called 'black box' effect consisting of the impossibility to reconstruct the steps from the beginning of the processing up to the final output.[178] Bathaee underlined that this issue current legal-regulatory approach to the black box problem, a right to receive an explanation 'poses an immediate threat to intent and causation tests that appear in virtually every field of law'.[179]

This scenario is made even more opaque and fragmented by the limits that Member States establish to these data subjects' rights.[180] Member State can restrict such rights to the extent that limitations are established by EU law or the Member State, provided that this restriction respects the essence fundamental rights and freedoms and a necessary and proportionate measure in a democratic society to safeguard interests such as, for example, national security.[181]

Within this framework, it is worth observing how, if, on the one hand, the rights to data subjects against automated processing can mitigate the interferences coming from processing of personal data through artificial intelligence technologies, on the other hand, the narrow scope of these rights could undermine the concrete enforcement of this safeguard, thus, increasing the possibility for data controllers to rely on automated decision-making technologies to process personal data. Nonetheless, the lack of legal certainty could also slow down the development of artificial intelligence technologies in Europe as we will examined in Chapter VII. Within this framework, the challenges of automated decision-making are another example of the clash between artificial intelligence and data protection, thus, pushing a constitutional interpretation of the GDPR which can explain the role of European data protection law in the algorithmic society.

---

[175] Working Party Article 29 (n 158), 21.
[176] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).
[177] GDPR (n 16), Recital 63.
[178] Pasquale (n 122).
[179] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology 890.
[180] Ibid, Art 23.
[181] Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35(5) Computer Law & Security Review.

5. A Digital Constitutional Approach to the GDPR

The analysis of the constitutional challenges for data protection in the algorithmic society shows the limits of European data protection law in relation to the exercise of powers through the implementation of artificial intelligence technologies for processing personal data. Nonetheless, a stand-alone reading of the GDPR can only provide a partial view. The relationship between artificial intelligence and GDPR, as a paradigmatic expression of European digital constitutionalism, cannot be understood without examining the role of constitutional law within this framework. As examined Chapter II, in the field of data, constitutional law has played a critical role in shifting the attention from an economic perspective to a fundamental rights system. Moving from the field of the law in the book to the law in action, it is worth observing how the ECJ played a fundamental role in the process of constitutionalisation of the right to data protection. The ECJ's judicial activism in the field of data protection shows how the relationship between fundamental freedoms and rights in the internal market is anything but equivalent. From the first recognition of data protection as a fundamental right in the *Promusicae* case,[182] even without emancipating this right from the safeguard of private life,[183] the ECJ reinforced the protection of this fundamental right as appears particularly clear in the decisions on digital privacy in the scenario following the entry into force of the Lisbon Treaty. The constitutional path of the protection of personal data reached a further step not only in the aftermath of Lisbon, but also with the adoption of GDPR whose first aim is to ensure the right to protection of personal data as data subjects' fundamental rights.[184]

The codification of a new approach in the GDPR is not enough to assess the degree of protection in the European context but needs to be framed within the European constitutional matrix. Both judicial emancipation and legislative consolidation have led the protection of the fundamental rights to privacy and data protection to be a global model on which European fortress of personal data is based as we will examine in Chapter VII. This is why the mere analysis of the GDPR can provide a short answer about the interpretation of European data protection law. Here,

---

[182] C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU (2008). Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* 3 (Springer 2009).

[183] Ibid. According to para 63: 'However, the situation in respect of which the national court puts that question involves, in addition to those two rights, a further fundamental right, namely the right that guarantees protection of personal data and hence of private life'. Juliane Kokott and Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.

[184] GDPR (n 16), Recitals 1-2. According to Recital 1: 'The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her'. According to Recital 2 GDPR: The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons'.

European digital constitutionalism can provide the normative lens to examine the relationship between algorithmic technologies and the GDPR. Therefore, it is time to analyse how digital constitutionalism can guide European data protection law which, despite the reach of a positive phase, needs to be framed within the framework of the asymmetry of power in the data field undermining fundamental rights and democratic values.

We can consider the GDPR as the positive expression of a new societal *pactum*. Such a regulatory outcome has been the result of the dominance of private actors over state actors competing in a context which is far beyond traditional national boundaries. It is no more enough to look at such fundamental rights in a negative vertical perspective thus binding just public actors to individuals but also as triggers of a positive responsibility to intervene at the horizontal level to remedy the asymmetry of power fostered by the algorithmic society. In other words, by translating constitutional values in legal principles and rights, the GDPR is an expression of the new phase of European digital constitutionalism. The GDPR breaks the vertical nature of fundamental rights, recognising individuals need to be protected by automated decision-making not only when performed by public actors but also by powerful private companies such as online platforms.

If we apply these considerations to data protection rules, we can understand how it is necessary to look at the European constitutional framework, precisely the constitutional values underpinning the GDPR, to understand the concrete scope of the relationship between artificial intelligence and European data protection law. The primary purpose of data protection law is to protect autonomy while ensuring transparency and accountability, and we have seen how the implementation of algorithmic technologies undermine these principles. As a result, the following subsections provide a teleological interpretation of the GDPR under the lens of digital constitutionalism. This approach would shed light on the constitutional values underpinning the GDPR and their impact on the processing of personal data through artificial intelligence technologies.

5.1 Human Dignity

The rise of the Internet has already shown how the social change triggered by this technology has revolutionised the public and private sector as well as individuals' daily lives. Artificial intelligence is promising to produce another shift of paradigm where the influence of individuals' rights is far from being irrelevant or merely linked to human beings. This does not mean that human would lose their role and replaced by machines. However, delegating decision-making without ensuring transparency could promote a framework where democratic values lose their attraction for society. This has been explained by Zuboff explaining how corporation have built a new form of (surveillance) capitalism based on the users' addiction to friendly technologies and under the logic of accumulation.[185] Processing data is the primary source to attract revenues within the framework of digital capitalism.[186] This process is guided by statistical models leaving correlation, and not causation, to define human characteristics. As underlined by Gutwirth and de

[185] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75.
[186] Jathan Sadowski, 'When Data Is Capital: Datafication, Accumulation, and Extraction' (2019) 6 Big Data & Society 1.

Hert, 'humans have become detectable, (re)traceable and correlatable'.[187] The personal data disseminated in daily lives are raw materials for artificial intelligence systems clustering humans within profiles determined by unaccountable systems based on correlation. This information is then used for making decisions on individuals which are unaware of this process unnoticeably affecting their autonomy, and, therefore, dignity.

Personal data are indeed 'personal' since they are part of data subjects' personality. They are not simply pieces of information. They can not only identify a natural person, but they can also provide a precise picture through the mix of some of the most intimate aspects of individuals like health or believes. From a European constitutional perspective, the importance of data are not just linked to marketability and the exchange in the internal market, but rather to a human dimension based on the protection of fundamental rights, with the result that we can think about data 'extra commercium'.[188] Personal data cannot be seen just as property rights. The 'propertisation' of personal data contributes to their commodification under the logic of digital capitalism with the result that any data would be considered as tradable as goods and not as piece of individuals' identity.[189] It is true that the circulation and exchange of personal data constitute the pillars of the information society. Nonetheless, the total commodification of personal data would lead to relying on private law and other legal regimes to deal with their commercial exploitation like copyright, consumer protection or contract law.[190] These concurring regimes would find their limits in the role of data as an expression of the individual and, therefore, personal data 'cannot be considered as a commodity'.[191] Likewise, the EDPS has underlined that personal data cannot be conceived as mere economic assets.[192] Even if human dignity is almost invisible in the GDPR,[193] as Floridi underlined, '"My" in my data is not the same as "my" in my car, but it is the

[187] Gutwirth and de Hert (n 182), 287.

[188] Václav Janeček and Gianclaudio Malgieri, 'Data Extra Commercium' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance—Contract Law 2.0?* 93 (Hart 2020).

[189] Giorgio Resta, *Identità personale e identità digitale* (2007) (3) Diritto dell'informazione e dell'informatica 511; Giorgio Pino, *Il diritto all'identità personale* (Il Mulino 2003); Lara Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano* (Giappichelli 2004); Guido Alpa, 'Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto all'identità personaleì (1989) (2) Giurisprudenza di merito 464; Stefano Rodotà, 'Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali' (1997) (4) Rivista critica diritto privato 558; Guido Alpa, Mario Bessone and Luca Boneschi (eds), *Il diritto all'identità personale* (Cedam 1981); Stefano Fois, 'Questioni sul fondamento costituzionale del diritto alla "identità personale"' in Guido Alpa and others (eds), *L'informazione e i diritti della persona* 159 (Jovene 1983).

[190] Yves Poullet, 'Data Protection Between Property and Liberties. A Civil Law Approach' in Henrik W.K. Kaspersen and Anja Oskamp (eds), *Amongst Friends in Computers and Law. A Collection of Essays in Remembrance of Guy Vandenberghe* (Kluwer Law International 1990), 160; Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011).

[191] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (2019) OJ L 136/1, Recital 24.

[192] European Data Protection Supervisor, 'Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (23 September 2016) <https://edps.europa.eu/sites/edp/files/publication/ 16-09-23_bigdata_opinion_en.pdf> 4 October 2020.

[193] GDPR (n 16), Art 88. This provision requires Member States to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context 'to safeguard the data subject's human dignity, legitimate interests and fundamental rights'. As Floridi underlined human dignity would be different from 'legitimate interests and fundamental rights' with the result that dignity would constitute an autonomous pillar underpinning the GDPR. Floridi (n 176).

same as "my" in my hand'.[194] Therefore, protecting the right to privacy should be considered as a matter of personal identity and integrity since they determine the evolution of human personality and therefore human dignity.[195] In a different way, the case of the right to be forgotten exactly shows this face of the right to privacy even before the rise of online platforms,[196] and the Google Spain case.[197]

The result of the commodification of personal data in the long run could be the slow fade of democratic values and the centrality of humans in society. The centrality of a human-centric approach in European data protection law comes from the ability of human dignity to permeate in the core of European fundamental rights. One of the primary characteristics of European data protection law is the intimate connection with individuals. The data subjects, as natural persons, are the core of the system. The notion of personal data extends far beyond the notion of identified natural persons. Without dealing with personal information, data protection law would not apply, thus, losing its legal meaning within the European framework. the scope of GDPR does not extend to legal persons or deceased.[198] The role of the individual is not only linked to the material scope of the GDPR. Such anthropocentric focus is not casual but comes from a frame of dignity characterising European constitutionalism.[199] The Charter opens up the catalogue of rights stating 'human dignity is inviolable. It must be respected and protected'.[200] The central position of this value within the Charter is not a formal recognition of constitutionality,[201] but it is the pillar of the entire system of the fundamental rights. This approach mirrors the Universal Declaration of Human Rights which enshrines human dignity in its preamble.[202] Therefore, despite the lack of axiology, human dignity should not be seen as a clashing value but as the core of each fundamental rights laid down in the Charter. As stressed in Chapter I, this is part of the European constitutional roots which looks at dignity as the pillar against any annihilation of humans.

Therefore, the mission of data protection law would be to ensure that its personalistic imprinting would not fall apart while ensuring democratic values of transparency and

---

[194] Floridi (n 176), 308.

[195] Antonio Ruggeri, 'Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)' (2016) (3) Consulta Online 371; Antonio Baldassarre, 'Il diritto di privacy e la comunicazione elettronica' (2010) (1) Percorsi costituzionali 49; Francesco Pizzetti, 'La tutela della riservatezza nella società contemporanea' (2010) (1) Percorsi costituzionali 61; Antonino Scalisi, *Il diritto alla riservatezza* (Giuffrè 2002); Tommaso Auletta, *Riservatezza e tutela della personalità* (Giuffrè 1978); Vittorio Frosini, 'Il diritto alla riservatezza' in Vittorio Frosini, *Il diritto nella società tecnologica* (Giuffrè 1981) 273; Vittorio Frosini, *La protezione della riservatezza nella società informatica* (1981) (1) Informatica e diritto 5; Adriano De Cupis, *Il diritto all'onore e il diritto alla riservatezza*, (Giuffrè 1948).

[196] Enrico Gabrielli (ed.), *Il diritto all'oblio* (Editoriale scientifica 1999); Giuseppe B. Ferri, 'Diritto all'informazione e diritto all'oblio' (1990) Rivista diritto civile 801; Tommaso Auletta, 'Diritto alla riservatezza e "droit a l'oubli"', in Guido Alpa and others (n 189), 127.

[197] Francesco Pizzetti (eds)*, Il caso del diritto all'oblio* (Giappichelli 2013); Massimiliano Mezzanotte, *Il diritto all'oblio. Contributo allo studio della* privacy *storica* (Editoriali scientifiche 2009); Franz Werro, 'The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash' in Aurelia Colombi Ciacchi and others (eds), *Liability in the Third Millennium, Liber Amicorum Gert Bruggemeier* 285 (Nomos 2009).

[198] Bart van der Sloot, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System' (2015) 31 Computer Law and Security Review 26.

[199] Catherine Dupré, *The Age of Dignity Human Rights and Constitutionalism in Europe* (Hart 2015).

[200] Charter (n 44), Art 1.

[201] Case C-377/98 Netherlands v European Parliament and Council (2001) ECR I-7079, 70-77.

[202] Universal Declaration of Human Rights (1948). 'Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world'.

accountability. This is not so far from the constitutional reasons triggering the positive dimension of the right to freedom of expression in the phase of digital constitutionalism as examined in Chapter V. The need to ensure that the core of fundamental rights is not compromised comes directly from the dignity of each individual not to experience the annihilation of its rights and freedoms. There would be no reasons to think about artificial intelligence as something abstracting human beings.

The focus of the GDPR on the data subject as individual can be examined from different perspectives beyond the notion of personal data. Still, data subjects' consent is the primary pillar of the data protection legal system, thus, representing the need to protect individuals' self-determination.[203] We have already seen in the first decision of the German Constitutional Court on data protection, such a freedom clearly emerge when dealing with the processing of personal data. In other words, it is the autonomous choice of the data subject which would allow the data controller to legally process personal data. This is why the GDPR also defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[204] However, consent could not always be an adequate legal basis since, in some case, the circumstances could not allow the data subject to express that or it has already shown to like when individuals enter into contracts whose data are necessary for its performance. This is why the GDPR provide exceptions to the rule of consent to lawfully process personal data, even when automated decision-making processes are involved.

Likewise, the double track of protection for personal data also aims to protect personal information which can reveal intimate aspects of human lives. Such a difference already introduced in the Data Protection Directive has been fostered by the GDPR which has extended the categories of data falling under the scope of such a special regime. It is interesting indeed that the GDPR ban the processing of these data even if it provides some conditions of lawfulness to process them.[205] For instance, biometrics and DNA data have been included within the broader protection of particular categories of data being information able to represent human as they are. Precisely, in a phase where biometric technologies are expanding and intertwining with artificial intelligence to pursue different tasks,[206] such a safeguard reflects the need to avoid that personal data are subject to automated decisions without the 'explicit consent' of data subjects. In this case, it is not enough to rely on the conditions for processing personal data, but it is necessary to ground the processing on specific legal bases.[207] Even in this case, the core of the entire system is the data subject's consent, which, in this case, should also be 'explicit'.

Such a personalistic approach also affects the framework of automated decision-making processing. The GDPR does not expressly clarify the constitutional values underpinning its structure. Therefore, a literal or systemic interpretation of data protection law could not provide a full picture of the values which the prohibition to subject individuals to these systems would protect. Dreyer and Schulz have underlined that the goal of this rule is beyond the mere protection

[203] Yves Poullet, 'Data Protection Legislation: What is at Stake for our Society and Democracy' (2009) 25 Computer Law & Security Review 211.
[204] GDPR (n 16), Art 4(11).
[205] Ibid, Art 9.
[206] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis* (Springer 2013).
[207] GDPR (n 16), Art 9(2).

of personal data.[208] Even if not exclusively, the primary goal of this rule is the protection of human dignity. The right not to be subject to automated decision-making deals with the ability of machines to make determinations about human lives. Even in this case, the rise of the Internet has shown how digital technologies can perform activities in a more efficient way than humans. The same is for artificial intelligence technologies able to see correlation that humans do not see or predict the future which is one of the abilities that humans have always try to reach.

What does not actually change, it is the risk of error. Even if machines could be more efficient of human, they can fail and reproducing the bias of their programmers. At first glance, algorithms would appear as neutral technology which can extract values from information that are useful for businesses and society. However, from a technical perspective, algorithms are far from being neutral technologies. They are not just mathematical models providing outcomes in a certain form based on the processing of information.[209] Algorithms transform inputs into outputs, thus, expressing a value judgement. Automated decision-making systems are therefore value-laden. The human role in the programming and development of these technologies contribute to reflect the bias and values of programmers into the technological design.[210] This is not a novelty since all technologies are the result of certain design choices. Reidenberg and Lessig have also shown how much the architecture of technology is a critical piece of the regulatory jigsaw.[211] In the case of algorithms, the role of design is even more critical since these technologies can produce decisions on which humans ground their activities.

Besides, scholars have underlined how machines are still not entirely able to interpret real dynamics and exactly understand contexts and emotions.[212] This limit also explains why so frequently, the implementation of artificial intelligence technologies has led to discrimination.[213] The right to equality can be considered another expression of human dignity. Without being considered equal, there are multiple layers of protection for different categories of 'humans'. The right to non-discrimination is one of the fundamental principles of European constitutional law. The right to equality is the basic pillar of constitutionalism as shown by its relevance in the Charter and the Convention.[214] Discriminatory outcomes of algorithmic processing can originate from the low level of data quality or embedded bias in the programming phase like in the case of discrimination based on ethnicity.[215]

---

[208] Dreyer and Schulz (n).

[209] Tarleton Gillespsie, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J. Boczkowski and Kristen A. Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* 167 (MIT Press 2014).

[210] Pasquale (n).

[211] Lawrence Lessig, *Code: And Other Laws of Cyberspace. Version 2.0* (Basic Books 2006); Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997-1998) 76 Texas Law Review 553.

[212] Andrew McStay and Lachlan Urquhart, 'This Time with Feeling? Assessing EU Data Governance Implications for Out of Home Emotional AI' (2019) 24(10) First Monday <https://firstmonday.org/ojs/index.php/fm/article/download/9457/8146> accessed 12 February 2020.

[213] Andrea Romei and Salvatore Ruggieri, 'A Multidisciplinary Survey on Discrimination Analysis' (2014) 29 The Knowledge Engineering Review; Bart Custers and others (eds), *Discrimination and Privacy in the Information Society* (Springer 2013); Kevin Macnish, 'Unblinking Eyes: The Ethics of Automating Surveillance' (2012) 14 Ethics and Information Technology 151.

[214] Charter (n 44), Art 20; Convention (n 39), Art 14.

[215] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

This is why the GDPR shield data subjects against the interference to their legal rights coming from the errors automated decision-making can produce. This prohibition would be indeed a recognition that machines cannot be fully trusted. In other words, such a rule clarifies that efficiency cannot prevail over fundamental rights and freedoms. At the same time, artificial intelligence technologies can also foster fundamental rights, thus, allowing humans to escape from marginalised environment. The GDPR has not banned this type of processing but tried to limit the serious effects that these technologies can produce on data subjects. This consideration also highlights why the GDRP has introduced the so-called human-in-the-loop principle. This is because humans' decisions cannot be affected by unaccountable automated systems but need another individual to assess them. This is firmly connected with the acknowledgement that machines err and are (still) not able to distinguish the complexity of human lives. As underlined by Floridi, humans are unique, precisely *hapax legomena*.[216] The attempts to digitised human lives to a mere calculation would annihilating the role of human in our society, leading towards a process of dehumanisation. In other words, the human being is *dignus*.[217] Any attempt to digitise humanity would clash with the nature of human beings.

Within this framework, human dignity is the primary beacon for data controllers and courts when focusing on the challenges of automated decision-making. This does not mean that this right should confer privacy and personal data quasi-absolute protection in any case. On the opposite, privacy and data protection would acquire a predominant role when there is the need to ensure that individual rights are not so compressed that autonomy and self-determination are effectively compromised. The limit established by the GDPR concerning the processing on automated decision-making processes is not a mere data subject right which can be overcome easily by ensuring security measures or opaque form of explanation. It is an instrument of freedom against the techno-determinism established by their machine and programmers coming from predominant private and public actors.[218] This rule horizontally connects human dignity, as the basic pillar of European constitutionalism, with artificial intelligence, thus, making the promises of algorithmic innovation more sustainable. The focus on human dignity would be the primary reference for lawmakers and judges in approaching this safeguard, thus, implying a strict interpretation of the exceptions and limitations to this 'human' right.

5.2 Proportionality

Human dignity is not the only underpinning value when looking at the relationship between artificial intelligence and the GDPR. Another constitutional value grounding European data protection is proportionality. The GDPR has indeed translated this principle which constitutes the foundation of the risk-based approach grounded on the principle of accountability. Like in the case of human dignity, different angles can show how this value is expressed by the GDPR and its relationship with artificial intelligence technologies.

---

[216] Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307.
[217] Stefano Rodotà, *Vivere la democrazia* (Laterza 2019).
[218] Antoniette Rouvroy, 'Technology, Virtuality and Utopia: Governmentality in an Age of Autonomic Computing' in Mireille Hildebrandt and Antoniette Rouvroy, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2011).

Proportionality is a pillar of democratic constitutionalism.[219] Even if this principle is declined in different ways on a global scale,[220] proportionality express the need to internally limit the exercise of public and private powers, thus, safeguarding individuals against excessive interferences.[221] European data protection law is a paradigmatic example of the principle of proportionality. As already stressed, personal data enjoy a broad margin of protection in the Union. However, at the same time, the protection of this fundamental right cannot lead to the destruction of other constitutional interests like freedom to conduct business as enshrined in the Charter.[222] Although the ECJ has recognised a high degree of protection to personal data, there is not a rigid hierarchy between fundamental rights and freedoms. Data protection is not an absolute right even when focusing on legitimate interests according to the tests established by the Convention and the Charter. Therefore, when interpreting the obligations of the GDPR, it is crucial not to forget that the interest of the data controller and the data subject represent nothing but the constitutional clash between the protection of personal data with other fundamental rights and freedoms or legitimate interests in the case of public authorities. In other words, the general principles, safeguards, and obligations of the GDPR need to be framed with such a context of balancing rather than axiology.

It is not by chance that this balancing approach is at the core of the GDPR's structure. Moving from the constitutional level to the GDPR, the principle of accountability of the data controller could be considered the constitutional translation of a risk-based approach based on the notion of balancing. The principle of accountability requires the controller to prove the compliance with GDPR's principles by establishing safeguards and limitations based on the specific context of the processing, primarily the risks for data subjects. The Data Protection Directive already had tried to introduce such an approach focused on the risk of processing, for instance, concerning the implementation of security measures.[223] Likewise, the WP29 stressed the role of a risk-based approach in data protection underlining how risk management is not a new concept in data protection law.[224] Even the Council of Ministers of the Organisation for Economic Cooperation and Development implemented a risk-based approach when revising the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, first adopted in 1980.[225]

From a formal perspective, despite the open clauses, the move from minimum to full harmonisation has been a powerful boost for legal certainty in the internal market. Such a move has not only led to strengthening the protection of privacy and personal data as fundamental rights of the Union but has also allowed a more balanced approach between rights and obligations. The

---

[219] Stephen Gardbaum, 'Proportionality and Democratic Constitutionalism' in Grant Huscroft and others (eds), *Proportionality and the Rule of Law. Rights, Justification, Reasoning* 259 (Cambridge University Press 2014).

[220] Alec Stone Sweet and Jud Mathews, *Proportionality Balancing and Constitutional Governance. A Comparative and Global Approach* (Oxford University Press 2019).

[221] Vicki C. Jackson and Mark Tushnet (eds), *Proportionality: New Frontiers, New Challenges* (Cambridge University Press 2017); Aharon Barak, Proportionality *Constitutional Rights and their Limitations* (Cambridge University Press 2012); Robert Alexy, *A Theory of Rights* (Oxford University Press 1985).

[222] Charter (n 44), Art 16.

[223] Kuner (n 82).

[224] Working Party Article 29, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (30 May 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/ wp218_en.pdf> accessed 30 January 2020.

[225] OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 22 February 2020.

principle of accountability reflects such a mix between certainty and proportionality. The data controller has been considered responsible (and not only liable) to ensure that the protection of data subject's privacy and data protection are ensured and protected. And this role comes from the respect not only of the GDPR's obligations but also general principles.

The GDPR modulates the obligation of the data controller according to the specific context in which the processing takes place,[226] namely 'taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural person'.[227] For instance, when looking at legitimate interest as conditions for lawfully process personal data, the GDPR provides a limitation balancing 'the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.[228] This focus extends also to the principle of privacy by design and by default as expression of the general principle of accountability.[229] As observed by Macenaite, 'risk becomes a new boundary in the data protection field when deciding whether easily to allow personal data processing or to impose additional legal and procedural safeguards in order to shield the relevant data subjects from possible harm'.[230] It would be enough to focus on the norms concerning the Data Protection Impact Assessment or the appointment of the Data Protection Officer to understand how the GDPR has not introduced mere obligations to comply but a flexible risk-based approach which leads to defining different margins of responsibility on each data controllers depending on the context at stake.[231] Fundamental rights are the parameters on which the risk-based approach based on a case-by-case assessment of data controllers' responsibility is based. This system represents nothing but the expression of a principle of proportionality reflecting the lack of a rigid axiology in the European constitutional framework. The risk-based approach reflects nothing else that the balancing of the conflicting interests of data subjects and controllers. In other words, the GDPR has led to the merge of a rights-based approach where the fundamental rights of data subjects play the role of beacon for compliance.

From the perspective of data controllers, the high standard of compliance required by the GDPR could however affect small or medium controllers which can be required to adopt higher safeguards, primarily when data processing operations could lead to high risks for the data subjects. This approach could affect the freedom to conduct business and development of the internal market. Even if the GDPR's approach could favour multinational corporations in the process of compliance, nevertheless, it introduces a mechanism which does not focus only on

---

[226] Raphael Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).
[227] GDPR (n 16), Art 24(1).
[228] GDPR (n 16), Art 6(1)(f).
[229] Ibid, Art 25. Ira S. Rubinstein, 'Regulating Privacy by Design' (2012) 26 Berkeley Technology Law Journal 1409; Ugo Pagallo, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* 331 (Springer 2012).
[230] Milda Maceinate, 'The "Riskification" of European Data Protection Law through a two-fold Shift' European Journal of Risk Regulation (2017) 8(3) European Journal of Risk Regulation 506.
[231] Working Party Article 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (4 October 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 4 October 2020. See Ruben Binns, 'Data Protection Impact Assessment: A Meta-Regulatory Approach' (2017) 7(1) International Data Privacy Law 22; Paul de Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in David Wright and Paul de Hert (eds), *Privacy Impact Assessment* 33 (Springer 2012).

rigid obligations but the concrete framework of the processing. This margin of discretion could promote the development of artificial intelligence technologies while protecting individuals' fundamental rights. This shift from theory to practice introduces certain flexibility allowing the data controller to determine the measures to apply according to the risks connected to data processing, while maintaining the duty to justify the reasons for these decisions. The GDPR would increase the discretion of the data controller in determining which safeguards apply to the data collected.

Likewise, from the data subjects' standpoint, the risk-based is complemented by a right-based system coming from the broad extension of fundamental rights in the European framework. Individuals have the right to access and limit the processing of their data, ask their erasure or portability based on the conditions established by the GDPR for each data subject's right. Scholars have underlined that 'from the user perspective, the impact of data portability is evident both in terms of control of personal data (and in general in the sense of empowerment of control rights of individuals), and in terms of a more user-centric interrelation between services. At the same time, it is a challenge to third data subjects' rights'.[232] This shows how the GDPR does not provide users with absolute rights. While empowering data subjects would increase the control over the processing of data, the implementation of their rights is a burden requiring data controllers to invest resources and define procedures to implement these rights.

When we frame such consideration in the field of artificial intelligence, we can observe that the GDPR does not establish an absolute prohibition in relation to automated decision-making, even if it bans the processing of particular categories of data except for the explicit consent of the data subject. The GDPR introduces exceptions according to which, despite potential legal or similarly significant consequences, data subjects cannot rely on this right. Their presence should not surprise when focusing on the characteristics of European constitutionalism do not recognise absolute protection to fundamental rights. As underlined by the ECJ, the right to the protection of personal data does not enjoy absolute protection but is subject to the balancing with other interests.[233] The protection of fundamental rights cannot lead to the 'destruction of any of the rights and freedoms recognised in this Charter or at their limitation to a greater extent than is provided for herein'.[234] In any case, limitations shall be strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality.[235] This is also shown by the exceptions that Member States can introduce to limit the right not to be subject to automated decision-making processes.[236]

Therefore, the principle of accountability is not only a burden for data controllers but also a threatening delegation of responsibility concerning the protection of fundamental rights and freedoms. In this way, the GDPR leads data controllers to become the arbiter of privacy and data protection. The limit to the exercise of this power is limited by the principle of proportionality which, together with human dignity, guides lawmakers and judges when addressing the balancing between data controller's accountability and data subject's fundamental rights. Therefore, the

[232] Paul de Hert and others, 'The Right to Data Portability in GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34(2) Computer Law & Security Review 193, 197.
[233] Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert (2010). See also GDPR (n 16), Recital 4.
[234] Charter (n 44), Art. 54.
[235] Ibid, Art 52.
[236] GDPR (n 16), Art 23.

principle of accountability can play an important role in the development of artificial intelligence technologies in the internal market without leaving fundamental rights behind. As a general principle, the more the discretion exercised by the data controller, the more the data subjects should be protected. This principle would leave data controller to perform their activities considering that their beacon of compliance is not just made by the GDPR's material and organisational requirements but the protection of individuals, precisely their dignity.

This is why the principle of human dignity is relevant within the framework of proportionality. Notwithstanding the GDPR's exceptions to data subjects' rights and freedoms would answer the need to balance conflicting interests, however, justifying exceptions to data subjects' rights against automated decision-making processes would betray the aim to protect human dignity. It would be worth wondering how exceptions could be tolerated in this case if these technologies could lead to a process of dehumanisation in the long run. The answer to such a concern can be found by looking at due process safeguards which would aim to preserve human dignity while promoting innovation.

5.3 Due process

The question is therefore how human dignity can be protected against potential disbalances in the exercise of conflicting rights and freedoms. Limitation to individuals' rights reflecting the principle of proportionality should not be considered as a threat to human dignity when due process safeguards are in place. The possibility to rely on procedural safeguards would mitigate disproportionate effects resulting from the exercise of public powers or private determinations. Due process would indeed play a crucial role even beyond the boundaries of public powers.[237]

Together with the personalistic principle, European data protection law is an example of due process safeguards. Since the adoption of the Data Protection Directive, European data protection law regulates the entire process of data processing from analysis of risks (e.g. DPIA), to rules on notice (e.g. mandatory disclosure), collection (e.g. consent), processing (e.g. purpose limitation), safeguards (e.g. data subject rights) and remedies (e.g. judicial enforcement). These norms represent the expression of the right to self-determination of individuals which, without knowing about how data are processed, cannot be aware of their personal information are used and, in the case of artificial intelligence, how data can lead to decisions involving legal rights. These ex-ante safeguards allow individuals to be aware of the existence of a process of automated decision-making as well as how it can generally influence its legal rights. Put another way, this approach would meet that principle of self-determination which makes humans *dignus* rather than subject to public and private determinations.

By promoting transparency and accountability in automated decision-making processes through procedural safeguards, the GDPR fosters human dignity. Therefore, due process is an essential tile of the constitutional mosaic of the GDPR. This is evident even when focusing on the safeguards relating to artificial intelligence technologies. The data controller is required to inform data subjects about the existence of a process of automated decision-making, its logic,

[237] Giacinto Della Cananea, *Due Process of Law Beyond the State: Requirements of Administrative Procedure* (Oxford University Press 2016).

significance and consequences,[238] and allow data subject to ask for accessing personal data.[239] In the case of the right not to be subject against automated decision-making, the GDPR recognises a procedural safeguard consisting of the right 'to require human intervention, to express her point of view and to contest the decision'.[240] Therefore, apart from when the processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, individuals have the right to ask for human intervention to assess the machine outcome.[241]

The principle of human-in-the-loop in the context of algorithmic decision-making is a paradigmatic example of due process. Several scholars underlined the need to guarantee minimal due process rights as an answer to the issue of asymmetry of power between individuals and data controllers in the context of automated decision-making.[242] This constitutional value raised within the realm of public actors is horizontally extended to the private actors through the obligation to ensure human intervention. It is not by chance that this principle is stated only when the processing involved automated decision-making technologies. This is because algorithmic decisions can produce serious effects on individuals' rights and freedoms, thus, deserving that the life of individuals' is not subject to determinations taken by unaccountable machines. To recover this lack of oversight on artificial intelligence, the GDPR requires that this processing deserves to be complemented by an adversarial principle and redress mechanism based on human intervention.

By recognising this right, the GDPR also seems to suggest that the last word over individuals' rights and freedoms should be human. A machine could not play this function without the support of humans that need to be in the loop. This is what the Commission already underlined in 1992 by observing that 'human judgment must have its place'.[243] This is why due process safeguards can protect human dignity complementing the general prohibition of full automated decision-making systems for the processing of personal data. This principle would break the efficiency characterising the evolution of technology. It does not just the recognise the role of humans in automate decision-making but also the primary of human assessment over the efficiency of machines. Paradoxically, the inefficiency and irrationality of human being is the last safeguard against the true interpretation of its nature.

The principle of human-in-the-loop cannot be considered as a general solution for the challenges raised by artificial intelligence. By looking to such a principle under the lens of proportionality, it can be observed that, while enhancing due process safeguards, it can potentially

[238] GDPR (n 16), Art 13.
[239] Ibid, Art 15.
[240] GDPR (n 16), Art 22(3). See Ben Wagner, 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11(1) Policy & Internet 104; Fabio M. Zanzotto, 'Viewpoint: Human-in-the-loop Artificial Intelligence' (2019) 64 Journal of Artificial Intelligence Research 243.
[241] Meg L. Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216.
[242] Danielle K. Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington University Law Review 1; Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 Boston College Law Review 93; Danielle K. Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.
[243] Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data COM(92)422 final, 26-27.

disregard other interests requiring protection. A broad extension of this rule can indeed undermine the freedom to conduct business or private actors or the performance of public tasks. Besides, as already stressed, relying on human intervention as a procedural safeguard does not ensure better decision-making.

These drawbacks are just a small price to pay to ensure that humans are not marginalised by opaque algorithmic technologies. These concerns are compensated by the critical role which due process plays against the unaccountable development of artificial intelligence technologies and the rise of private powers in the algorithmic society. The development of automated systems is not always driven by public purposes but usually business interests focused on profit maximisation. Design choices are not neutral but answer to opaque business logic which transforms human life in technical norms of processing and extraction of values. In other words, they define transnational standards of automated systems outside any public scrutiny, thus, creating a para-constitutional environment competing with public values. This situation is not only relevant for due process, but also for the principle of the rule of law. If legal norms are replaced by technological standards, there will be no space for democratic constitutionalism to ensure the protection of public values against the rise of unaccountable technologies expressing private powers. Within this framework, the principle of human-in-the-loop is a shield not only as a due process safeguard, but also to protect democratic values.

The GDPR is fostering the principle of the rule of law when the processing of personal data involves automated decision-making. In this way, the GDPR bans any discretionary use of automated decision-making to process personal data. The principle of the rule of law is a critical value to reduce the gap between the public and private sector involved in processing personal data. In the lack of any legal obligations, private actors are not required to explain to reasons justifying their policy or actions. While public actors are required to comply with constitutional principles, the private sector would not be bound by constitutional principles and norms without a positive translation as it occurred with the GDPR. In the algorithmic society, private companies have shown their abilities to acquire dominant positions in the market of data by extracting value from them. Within this framework, the data subject could be considered as a vulnerable actor whose protection of rights and freedoms should find its ground not only in substantive rights but also procedural safeguards to remedy the imbalance of power.

Within this framework, the principle of due process complements the relevance of human dignity and proportionality as the expression of the constitutional values underpinning the GDPR. In this case, the GDPR obligations should not be seen as mere instruments for requiring data controllers to comply with certain rules but as the constitutional expression of procedural safeguards aimed to avoid the disproportionate exercise of powers in the balancing between conflicting interests. In this sense, the obligations of the GDPR should be constitutionally interpreted as a mean to ensure that human dignity and democratic values are not annihilated by the lack of transparency and accountability in the exercise of powers in the field of data.

6. Humans in the Algorithmic Society

The implementation of artificial intelligence technologies in the processing of personal data has increased the concerns for individuals subject to ubiquitous forms of control and surveillance and democratic values. The role of artificial intelligence for the fourth industrial revolution is not only

relating to the potentialities of these technologies but, like for the Internet at the end of the last century, to its dissemination in the society and commodification.[244] These technologies are no longer closed to the domain of academics or specific business sectors, but they are spreading by reaching consumers, especially because of the need to gather data and information to train artificial intelligence technologies which can provide new models and predictive answers. One of the primary promises of artificial intelligence is helping human to decide, for example, by replacing or solving complex questions through data analytics.[245]

At the same time, we have seen how data protection law emerged as an answer to the challenges of automation. Automated technologies triggered the emergence of data protection as a new and autonomous fundamental right in the European framework. The constitutional evolution of data protection in the European framework shows the relevance of this fundamental right for safeguarding democratic values in a society which has strongly digitised in the last forty years. Since 1995, the role of the ECJ has underlined a shift from an economic perspective linked to the growth of the internal market to a constitutional approach which has led to the adoption of GDPR in 2016.

The potentialities of artificial intelligence challenge the right to privacy once again and require data protection to do a step forward. The broad notion of personal data and the clash between artificial intelligence and the GDPR's general principles introduce a relevant layer of complexity for data controllers. Likewise, the limits to the use of automated decision-making could challenge the smooth development of artificial intelligence technologies in the internal market. As already addressed, this situation is the result of the European process of constitutionalisation leading the protection of individuals' fundamental rights to be the beacon of data protection law.

Despite these challenges, the characteristics of European digital constitutionalism can provide an interpretative path to understand the role of data protection law in the algorithmic society. The GDPR has led to the translation of constitutional values which are not only focused on the protection of privacy and data protection as fundamental rights. The GDPR has also horizontally extended to the private sector other constitutional values, precisely, human dignity, proportionality, and due process. In this way, European data protection law can play its role as a safeguard for the right of privacy and self-determination while breaking the asymmetries of powers threatening democratic values.

Therefore, the rise and consolidation of European data protection has not led to a mere evolution of the constitutional paradigm but a translation of constitutional values into operational norms. This approach would allow not to lose the centrality of human dignity and protect individuals against opaque and unaccountable processing of personal data in the hands of powerful actors like public actors or private businesses like online platforms. Nonetheless, the role of digital constitutionalism is far from being exhausted. A new phase of digital constitutionalism is likely around the corner to answer the challenges of the algorithmic society.

---

[244] Brandon Allgood, 'The Commoditization of AI and The Long-Term Value of Data' Forbes (10 April 2017) <https://www.forbes.com/sites/forbestechcouncil/2017/04/10/the-commoditization-of-ai-and-the-long-term-value-of-data/#74c71abd159c> accessed 26 July 2019.

[245] Brian Cantwell Smit, *The Promise of Artificial Intelligence. Reckoning and Judgment* (MIT Press 2019).

Chapter VII

The Road Ahead of European Digital Constitutionalism

Summary: 1. Towards a Fourth Phase? – 2. Values: Digital Humanism v Digital Capitalism. – 3. Governance: Public Authority v Private Ordering. – 4. Scope: Constitutional Imperialism v Constitutional Protectionism. – 5. Conclusions: The Constitutional Lesson Learnt and the Digital Road Ahead.

1. Towards a Fourth Phase?

The European path towards digital constitutionalism has led to a change of paradigm where the expansion of liberal goals of the internal market has met a new (digital) constitutional approach. The liberal narrative characterising the Union's policy at the beginning of this century have slowly faded away before the lights of a new constitutional moment. As examined in Chapter II, the digital liberal approach adopted at the end of the last century has been slowly replaced thanks to the ECJ's judicial lessons and the consolidation of the European constitutional order in the aftermath of the Lisbon Treaty. The second phase of judicial activism has paved the way towards the constitutional reaction characterising the third (constitutional) phase opposing the troubling rise and evolution of private powers online.

At the dawn of a new digital constitutional moment in Europe, it is worth wondering towards which directions the promising evolution of artificial intelligence technologies will lead the Union in the next years.[1] The Union has already shown its commitment to be an active part of global dynamics.[2] In her political guidelines, Commission President von der Leyen underlined the two political branches guiding the Union in the next decades to ensure the transition to a healthy planet and a new digital world. These two drivers cannot be considered as isolated but complementary.[3] The European Green Deal underlines the need for an immediate turning point towards sustainable solutions which are resource-efficient, circular and climate-neutral.[4] Besides, such green goals require to be complemented by the benefits coming from the evolution of the digital society.[5] The Data Strategy aims to establish the creation of a 'single European data space'.[6] It consists of ten

[1] Mireille Hildebrandt, 'The Artificial Intelligence of the European Union' (2020) 21 German Law Journal 73.
[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2020. A Union that strives for more, COM(2020) 37 final.
[3] Luciano Floridi, 'The Green and the Blue: Naïve Ideas to Improve Politics in a Mature Information Society' in Carl Öhman and David Watson, *The 2018 Yearbook of the Digital Ethics Lab* (Springer 2018), 183.
[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal, COM(2019) 640 final.
[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67 final.
[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy for data, COM/2020/66 final.

sectoral common European data spaces which are relevant for twin green and digital transitions. Likewise, the White paper on artificial intelligence is another piece of the European strategy.[7] The mix between environment and technology is critical even when considering the UN Sustainable Development Goals.[8]

The rush for artificial intelligence fits exactly within this global challenge. China is approaching to be the world leader in the field of artificial intelligence technologies by 2030,[9] with its R&D sector which might match that of OECD by 2020.[10] Whereas, the US tech giants dominate digital markets and continue to extend their power to other sectors.[11] The role of artificial intelligence for the fourth industrial revolution is not only relating to the potentialities of these technologies but its dissemination in the society and commodification.[12] These technologies are no longer closed to the domain of academics or specific business sectors, but they are spreading by reaching consumers, especially because of the need to gather data and information to train artificial intelligence technologies. This promising scenario can lead to new opportunities,[13] thus, promoting the growth and competitiveness of the internal market in the international arena. At the same time, if, on the one hand, artificial intelligence technologies provide new opportunities for the Union, on the other hand, they also pose relevant challenges for society,[14] especially concerning fundamental rights and democratic values.[15]

We have already seen how the evolution of the digital environment and the first application of algorithmic technologies have led to adopting a liberal approach to protect innovation which challenged fundamental rights and freedoms while leading to the rise of new digital powers. Unlike at the end of the last century, the rise of digital constitutionalism has provided a first reaction, thus, creating the grounds on which the Union can build its strategy in the next years to avoid that constitutional values slowly fade away in the name of innovation or logics outside democratic channels. However, as stressed in Chapter V and VI, there is still much work to be done. Artificial intelligence has already raised new challenges even if we are still at the dawn of this phenomenon. This is why the rise of digital constitutionalism looks far from being a point of arrival as the last step of the European constitutional path.

It would be already possible to frame evolving trends leading the European constitutional

---

[7] White paper, 'On Artificial Intelligence - A European Approach to Excellence and Trust' COM(2020) 65 final.
[8] UN General Assembly, Resolution adopted by the General Assembly on 25 September 2015 A/RES/70/1 (2015).
[9] Will Knight, 'China Plans to Use Artificial Intelligence to Gain Global Economic Dominance by 2030' MIT Technology Review (21 July 2017) <https://www.technologyreview.com/2017/07/21/150379/china-plans-to-use-artificial-intelligence-to-gain-global-economic-dominance-by-2030/> accessed 4 July 2020.
[10] OECD, 'China appears on course to match OECD R&D intensity by 2020' <http://www.oecd.org/sti/DataBrief_MSTI_2018.pdf> accessed 4 July 2020.
[11] Nick Srnicek, *Platforms Capitalism* (Polity Press 2016).
[12] Brandon Allgood, 'The Commoditization of AI and The Long-Term Value of Data' Forbes (10 April 2017) <https://www.forbes.com/sites/forbestechcouncil/2017/04/10/the-commoditization-of-ai-and-the-long-term-value-of-data/#74c71abd159c> accessed 26 July 2019.
[13] Brian Cantwell Smit, *The Promise of Artificial Intelligence. Reckoning and Judgment* (MIT Press 2019).
[14] Sue Newell and Marco Marabelli, 'Strategic Opportunities (and Challenges) of Algorithmic Decision-making: A Call for Action on The Long-Term Societal Effects of 'Datification' (2015) 24 The Journal of Strategic Information Systems 3.
[15] Filippo Raso and others, 'Artificial Intelligence & Human Rights: Opportunities & Risks' (2018) Berkman Klein Center Research Publication No. 2018-6.

strategy before some dilemmas. Firstly, automated decision-making technologies developed by transnational actors are promising new opportunities for growth and innovation. Like at the end of the last century, this promising scenario could trigger neoliberal approaches, thus, consolidating the path of digital capitalism. At the same time, these technologies have already shown to challenge the protection of fundamental rights and freedoms undermining the role of human dignity in the algorithmic society. Therefore, the first dilemma is a matter of values in the algorithmic society (digital humanism v digital capitalism). Secondly, it is worth focusing on the governance of these values. The mix of public authority and private ordering contribute to shaping the evolution and implementation of artificial intelligence technologies. The dilemma between hard and self-regulation or the cooperation between the public and private powers are some of the primary challenges for constitutional democracies in the information society (public authority v private ordering). Thirdly, the global spread of algorithmic technologies would lead to focus on the scope of these values and their governance at the intersection between public and private actors. While the traditional characteristics of sovereign powers would limit the application of rights and freedoms to a certain territory, private actors can extend their standards globally. Precisely, the attempts of public actors to extend the protection of fundamental rights beyond territorial boundaries could be a solution to mitigate the influence of global standards developed by unaccountable private entities. At the same time, the limits to the exercise of sovereign powers beyond territorial boundaries could encourage democratic constitutional states to look at global phenomena with scepticism in order to protect constitutional values from the interferences of global private values (constitutional imperialism v constitutional protectionism).

Within this framework, this chapter argues that the characteristics of European digital constitutionalism would lead to constitutional paths escaping polarisation. The primary goal of this chapter is to underline how the talent of European constitutional law would not promote a constitutional approach leading to sustainable growth of the internal market while protecting fundamental rights and democratic values in the long run. The first part of this chapter focuses on the dilemma between digital humanism and digital capitalism underlining the potential path characterising the European approach to artificial intelligence technologies. The second part examines how European constitutional law would lead to a third way between public authority and private ordering. The third part underlines to what extent the Union would likely extend the scope of its constitutional values to address the global challenges of artificial intelligence technologies. Once this chapter underlines the potential road ahead of European digital constitutionalism, the fourth part summarises the primary findings of this work.

2. Values: Digital Humanism v Digital Capitalism

The rise of the algorithmic society has triggered a new wave of opportunities for the growth of the internal market. The processing of data has become an integral part of the public and private sector. Whilst, in the last century, the potentialities of artificial intelligence could not bring out due to the lack of a vast amount of interconnected data to process leading to the so-called 'AI winters',[16] today, the evolution of global communication technologies allowing the storing and

[16] Luciano Floridi, 'AI and Its New Winter: From Myths to Realities' (2020) 33 Philosophy & Technology 1.

exchanging information seems to promise a different path in the consolidation and implementation of these technologies in daily lives.

New automated processing techniques fostered by the availability of large datasets have led to a sharp increase in the number of intelligent products and services. Although automated systems are still in the phase of 'narrow AI', significant improvements have been achieved, for example, in the analysis and prediction of human behaviour and characteristics, or in the field of robotics.[17] From banking and insurance to the medical sector, automated decision-making technologies offer new possibilities of prediction and interpretation of reality based on a different degree of determinism like neural networks. One example consists of biometric technologies where voice and facial recognition are not only implemented by public authorities for the performance of public tasks like border control.[18] Even the private sector processes biometric data, primarily to profile individuals for business purposes.[19]

This is why artificial intelligence looks like an opportunity for the internal market and, more generally, the driver of the fourth industrial revolution. Data are the fundamental asset for the digital economy due to their capacity to generate value. At the same time, Chapter V and VI have shown how automated technologies have highly challenged the protection of fundamental rights and democratic values. The development of these technologies provides interesting opportunities to perform public tasks and achieve business goals, but, at the same time, automated decision-making can lead to constitutional concerns. Discriminatory results, biased decisions, censoring speech or subject users to forms of surveillance are only some examples of the values at stake.[20] Health and security, privacy and self-determination, speech and discrimination, are values involved in processes of decision-making outside human judgement or oversight. When looking at this scenario, we meet a crossroads between a model where individuals' rights and freedoms are shielded against the appeal and promise of new technologies (i.e. digital humanism) and a neoliberal view looking at the new opportunities of artificial intelligence technologies as a potential engine for economic growth and individual autonomy (i.e. digital capitalism).

This would not be the first time that constitutional democracies face this dilemma. If we turn back and look at the last twenty years, we have seen how the Union has moved from the economic pole based on a digital liberal approach coming from the US neoliberal paradigm to a mature approach which takes into high consideration the protection of fundamental rights and democratic values in the information society. At the end of the last century, there were not so many clues to look at the rise of digital capitalism as a potential challenge for constitutional democracies. Nonetheless, this liberal approach has been exactly the constitutional ground for the evolution of digital powers against which European digital constitutionalism has reacted. In Chapter V and VI, we have seen the role of European constitutional law, and precisely human dignity, in promoting new positive approaches in the field of content and data. The rise of a new phase of digital

[17] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 UC Davis Law Review 399.
[18] Paul de Hert, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Patrizio Campisi, *Security and Privacy in Biometrics* 369 (Springer 2013).
[19] Lauren Stewart, 'Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security' (2019) 60 Boston College Law Review 347.
[20] David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Polity Press 2018).

constitutional is indeed the natural reaction of European constitutional law to the threats of digital capitalism.

Human dignity would mitigate potential threats of techno-determinist solutions that could lead to processes of dehumanisation and gradually vanishing of democratic values. According to the European Data Protection Supervisor, '[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. [...] Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing'.[21] There are strong ethical and legal concerns brought by the rise of the algorithmic society like the autonomy of robots, online censorship and trust in automated decision-making processes.[22] Digital ethics is at the centre of the European policy response to the challenges raised by artificial intelligence technologies in terms of liability, safety, the internet of things (IoT), robotics, algorithmic awareness, consumer and data protection.

It should not come as a surprise that a human-centred approach is the core of the European strategy to artificial intelligence. In 2018, the Commission appointed a new High-Level Expert Group on Artificial Intelligence whose published its artificial intelligence ethical guidelines.[23] The group underlined the importance of adopting a pan-human approach to these technologies which looks at human dignity as the common foundation of European fundamental rights and values according to which 'the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields'.[24] The same approach is also reflected in the strategy of the Union on artificial intelligence.[25] The white paper on artificial intelligence expressly clarifies that '[g]iven the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'.[26] The Council of Europe underlined that '[c]onscious therefore of the evolving impact, which may be positive or negative, that the application of algorithmic systems with automated data collection, analytics, decision making, optimisation or machine learning capacities has on the exercise, enjoyment and protection of all human rights and fundamental freedoms, and of the significant challenges, also for democratic societies and the rule of law, attached to the increasing reliance on algorithmic systems in everyday life'.[27]

From this perspective, the Union seems to take a precise path towards digital humanism. A closer look can reveal how the Union has not entirely closed its door to digital capitalism. It is true that, at first glance, protecting rights and democratic values against a reckless race to innovation towards dehumanisation would be one of the aims of European constitutionalism.

---

[21] European Data Protection Supervisor, 'Opinion 4/2015. Towards a new Digital Ethics' (11 September 2015) <https://edps.europa.eu/ sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 6 July 2020.
[22] Mark Coeckelbergh, *AI Ethics* (MIT Press 2020).
[23] High-Level Expert Group, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 28 September 2020.
[24] Ibid, 10.
[25] COM(2020) 65 (n 7).
[26] Ibid, 2.
[27] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (8 April 2020) <https://www.statewatch.org/media/documents/news/2020/apr/coe-recommendation-algorithms-automation-human-rights-4-20.pdf> accessed 7 October 2020.

Nonetheless, the situation is more nuanced than it could appear at first glance. The European constitutional safeguards could be seen as limits to the development of new technologies and, therefore, be a competitive disadvantage vis-à-vis other global technological poles, like China or the US. As examined in Chapter V, the Union has adopted a more restrictive approach to the power of online platforms over content. Precisely, the Union has focused on shaping the boundaries of online platforms' responsibilities in Europe by introducing a mix of hard and soft law measures to tackle the spread of illicit content. A first positive reaction of the Union has led to remedying the discretionary interferences to users' freedom of expression. Likewise, in Chapter VI, we have underlined the role of data protection in limiting the discretionary development of automated decision-making technologies. The GDPR has constituted a step forward in counterbalancing and preventing disproportionate interferences with individuals' personal data and, therefore, autonomy and dignity. In this sense, the GDPR plays a constitutional function limiting the rise of private powers in the algorithmic society. Put another way, the GDPR can be considered as the horizontal translation of a mix of constitutional values characterising European constitutionalism.

These limits to safeguard fundamental rights and democratic values would not raise concerns if the Union was the only actor participating in the run towards artificial intelligence technologies around the world. These safeguards can hinder the smooth development of new technologies. Granting extensive protection of fundamental rights over innovation could lead the Union to become a 'standard-taker' rather than a 'standard-maker' in the field of artificial intelligence. It would be enough to focus the broad constitutional protection recognised to personal data in the European context to argue, at least apparently, a competitive disadvantage of the Union vis-à-vis other countries where the safeguards of data protection law are not equivalent. Since granting 'extensive protection of data privacy rights restrains the use of AI's most useful features: autonomy and automation',[28] one of the most important challenges for the Union in the fourth industrial revolution is to understand where to draft a line between innovation and risk.

Since the role of artificial intelligence for the fourth industrial revolution, this is not a trivial constitutional issue. A lower degree of guarantees and safeguards can constitute a competitive advantage in the market of artificial intelligence. This could trigger a rush to the bottom in the protection of fundamental rights in order not to suffer of a competitive disadvantage. It cannot be excluded that the fight in the international arena for becoming the standard maker in the field of artificial intelligence could lead to a dangerous reduction to democratic and constitutional safeguards in the name of innovation. The potential technological *subjectionis* of the Union driven by extensive protection of individuals' fundamental rights could lead to the extension of technological paradigms of protection coming from areas of the world which does not ensure adequate safeguards for users and society at large. Put another way, the constitutional advantage in the short term could lead Europe in a situation of *de facto* technological disadvantage due to the need to rely on technologies developed in areas of the world where the lack of restrictions and liberal approach leaves the development of unaccountable models of governance. This would lead to the extension of external paradigms of protection which would influence European values due to the need to be competitive in a global market.

[28] Matthew Humerick, 'Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2018) 34 Santa Clara High Technology Law Journal 393, 412.

Within this multifaceted framework, the primary challenge concerns what kind of innovation the Union wants to achieve and whether this choice is based on a liberal approach reducing the scope of safeguards in the name of innovation. Therefore, the question would be whether, in this bipolar system made of opportunities and challenges, European digital constitutionalism could provide a third way avoiding liberal approaches like at the end of the last century without recognising an almost degree of protection to fundamental rights. The position of the Union in this field is peculiar due to the role of the two technological poles, precisely China and the US, which are currently leading the fourth industrial revolution.[29] In this geopolitical scenario, the Union has shown its intent to be a crucial player in this match.[30] However, the Union has strongly underlined the ethical, economic and legal impacts which the implementation of artificial intelligence technologies can produce on society.[31] Although the Union is aware of the potentialities of these technologies and the need to be competitive in the international arena, the protection of personal data together with the compelling need to protect democratic values against the threats raised by artificial intelligence technologies could constitute a 'constitutional brake' limiting the flourishing of these technologies.

Despite this consideration, the Union has not totally abandoned its economy roots.[32] It should not come as a surprise if the Union agenda already showed its commitment to build a Digital Single Market Strategy,[33] and the establishment of an ethical and legal strategy for artificial intelligence and data.[34] To benefit from the full potentialities of this new technological framework, it is necessary to invest resources and ensure the smooth development of these technologies without hindering innovation. In the mid-term review of the Digital Single Market strategy, the Commission highlighted the importance of being in a leading position in the

[29] Klaus Schwab, *The Fourth Industrial Revolution* (Crown 2016); Daniel Araya, 'Governing The Fourth Industrial Revolution' Forbes (12 May 2019) <https://www.forbes.com/sites/danielaraya/2019/03/12/governing-the-fourth-industrialrevolution/#4eea13a14b33> accessed 21 August 2019.

[30] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions, Artificial Intelligence for Europe COM(2018) 237 final.

[31] High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> accessed 29 August 2019.

[32] Sophie Robin-Olivier, 'The 'Digital Single Market' and Neoliberalism: Reflections on Net Neutrality', in Margot E. Salomon and Bruno De Witte (eds), *Legal Trajectories of Neoliberalism: Critical Inquiries on Law in Europe* 45 (Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2019/43, 2019).

[33] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe (COM/2015/192 final).

[34] See for example, the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL); European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)); Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, COM(2018) 237 final; Declaration of cooperation on Artificial Intelligence, signed by EU Member States <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence> accessed 26 June 2018; Draft AI Ethics Guidelines 'Artificial intelligence, real benefits' <https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai> accessed 18 December 2018; Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence COM(2018) 795 final.

development of artificial intelligence technologies.[35] It underlined the importance for the Union to benefit from the opportunities of these technologies through a three-pronged approach: increasing public and private investment; preparing for socio-economic changes brought about by artificial intelligence; and ensuring an appropriate ethical and legal framework.

The Union has shown its intention not to become a mere follower of other technological poles rather than a standard maker in the field of content. The Union has mitigated the discretion of the private sector to determine how to tackle illicit content (e.g. code of conduct on hate speech). Besides when looking at the Digital Services Act package, the trend is not only towards increasing responsibilities of online platforms and certainty in the moderation of content but also to ensure fair competition and promote the development of small and medium-size businesses.[36] Moving to the field of data, while the GDPR increases the degree of protection for individuals' fundamental rights, other aspects promote the processing of personal data in the business sector and leaves some areas of governance to the private sector. In this case, the GDPR can be considered a regulation of surveillance capitalism which does not impede tech giants to collect and process data but regulate this process.

This mix between innovation and the protection of individuals' fundamental rights is not just the result of regulatory choices, but reflects the characteristics of European constitutionalism where the need to balance different fundamental rights could not lead digital humanism or digital capitalism to entirely prevail over each other. The constitutional protection of freedom of expression, privacy and personal data requires to take into consideration not only how to safeguards to fundamental rights but also other conflicting interest such as the freedom to conduct business. At the same time, the freedom to conduct business or the aim to achieve the goals of the internal market cannot lead to the annihilation of fundamental rights and freedoms. European constitutional law is not prone to recognise absolute protection to constitutional values which would lead to the destruction of other conflicting interests.

Therefore, European digital constitutional would lead towards a hybrid approach between digital humanism and capitalism. This European 'third way' should not be considered just a political choice but the result of the natural tendency of European constitutionalism not to take a polarised position but put together the different constitutional pieces of the puzzle in a dialectic form. The Union does not aim to leave its businesses free to develop new technologies under a neoliberal scheme like in the US or strongly intervene in the market to support the development of new technologies and businesses like in the case of China. As we will underline in the next sections, the Union is rising as a global regulator driven by a constitutional approach whose beacon is constituted by the principle of human dignity. This is something belonging to the nature of the Union since it is 'founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'.[37]

In front of the crossroads between digital humanism and capitalism, the Union seems to have chosen a path towards the development of a sustainable artificial intelligence environment rather than focusing just on fostering innovation to exploit the potentialities of these technologies or merely impeding their development. Notwithstanding the Union approach could be subject in the

[35] COM(2018) 237 final (n 34).
[36] LIBE, on the Digital Services Act and Fundamental Rights Issues Posed (2020/2022(INI)).
[37] Consolidated version of the Treaty on European Union (2012) OJ C 326/13, Art 2.

short term to a competitive disadvantage in the field of artificial intelligence, in the long term, the European approach could promote a human-centric development of artificial intelligence technologies. As stressed by the Commission, 'Given the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'.[38] Put another way, against a fierce global competition in the field of artificial intelligence and considering its relevance for the future of Europe, the Union has chosen to promote the development of these technologies without forgetting the protection of rights and freedoms.

Once we underline the value characterising the Union approach, the second point consists of focusing on the governance of these values. It is worth wondering how the Union would concretely put in place its strategy at the intersection between digital humanism and digital capitalism. In order to ensure that technology does not order society and human beings, but it is functional to the evolution of mankind, it is critical to wonder about the relationship between the exercise of public authority and private ordering, precisely between the role of law and self-regulation. Choosing one of the two poles in the algorithmic society is not a neutral choice. As underlined in Chapter V and VI, the private governance of content and data in the digital environment left individuals at the margins and subject to ubiquitous private systems influencing their decisions without being able to understand or control the technologies and, therefore, to participate consciously in a democratic society. Therefore, the primary challenge is how citizens can ensure that constitutional values underpinning their social contract are not left to unaccountable determinations outside democratic circuits. This is a question concerning the governance of values in the algorithmic society. As underlined by the Council of Europe, 'ongoing public and private sector initiatives intended to develop ethical guidelines and standards for the design, development and ongoing deployment of algorithmic systems, while constituting a highly welcome recognition of the risks that these systems pose for normative values, do not relieve Council of Europe member States of their obligations as primary guardians of the Convention'.[39] Rather than proposing a self-regulatory approach, European digital constitutionalism is increasingly pushing towards the role of public actors in ensuring a framework of values guiding the development of artificial intelligence technologies. The next subsection underlines how finding a point of balance between the exercise of public authority and private ordering would be critical to promote the sustainable and democratic development of artificial intelligence technologies.

3. Governance: Public Authority v Private Ordering

'People are entitled to technology that they can trust. What is illegal offline must also be illegal online. While we cannot predict the future of digital technology, European values and ethical rules and social and environmental norms must apply also in the digital space'.[40] This political statement underlines the importance of the European values in the development of digital

[38] COM(2020) 65 final (n 7), 2.
[39] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems <https://search.coe.int/cm/pages/result_details.aspx?objectid =09000016809e1154> accessed 2 July 2020.
[40] COM(2020) 67 final (n 7), 10.

technologies. However, defining values is just one step. Individuals are increasingly surrounded by ubiquitous systems whose values are governed by private actors. The positive consequences of the spread of artificial intelligence firmly clash with the troubling opacity of 'algocracy'.[41] Leaving algorithmic technologies without any democratic safeguard would lead to open the way to a form of techno-determinism, allowing private actors governing algorithmic technologies to autonomously determine the standard of protection of rights and freedoms on a global scale. The Council of Europe underlined that 'bearing in mind that digital technologies hold significant potential for socially beneficial innovation and economic development, and that the achievement of these goals must be rooted in the shared values of democratic societies and subject to full democratic participation and oversight'.[42] Therefore, in order to protect democratic values while promoting innovation, defining the governance of artificial intelligence technologies is a critical piece of the puzzle. Put another way, the Union's choice at the intersection between digital humanism and digital capitalism needs a system of governance which can ensure the effective implementation of the European democratic approach to the algorithmic society.

As examined in Chapter III, transnational private actors have consolidated delegated and autonomous areas of powers while privately ordering the fields of content and data. The rise of European digital constitutionalism can also be read as a reaction against the power of online platforms to discretionary establish their values on a global scale. Content moderation and individuals' profiling are two examples of how private actors have been able to rely on a self-regulatory framework driven by business logics rather than public values. While, at the end of the last century, the primary concern was not overwhelming the private sector with regulatory burdens, now, the Union is showing to be concerned about the dramatic shift from public values to private determination driven by profit maximisation. The rise of digital capitalism is nothing else that the fruit of a digital liberal approach which has not considered how leaving private actors without a framework of safeguards and oversight could affect society at large and lead to concentration of new powers.

The European commitment not to be subject to the logic of digital capitalism is evident. The European orientation to digital ethics shows that the market cannot autonomously prevail over the need to safeguard fundamental rights and democracy. Ethics could play a critical role in the governance of artificial intelligence.[43] Nonetheless, the extensive reliance on solutions based on ethics and self-regulation could not solve the current situation of asymmetry of power in the algorithmic society. The predominance of ethics over the law could build a neoliberal narrative diluting the role of regulation over self-regulation, thus, leading the private sector to define what is good behaviour or, more precisely, objectionable conducts online. Even if companies share

[41] John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 Philosophy & Technology 245.
[42] CM/Rec(2020)1 (n 39).
[43] Coeckelbergh (n 22); Johanna Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation' in Markus D. Dubber, Frank Pasquale, and Sunit Das (eds), *The Oxford Handbook on Ethics of AI* (Oxford University Press 2020); Virginia Dignum, *Responsible Artificial Intelligence* (Springer 2019); Luciano Floridi and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28(4) Minds and Machines 689; Nick Bostrom and Eliezer Yudkowsky, 'The Ethics of Artificial Intelligence' in Keith Frankish and William M. Ramsey (eds), The Cambridge Handbook of Artificial Intelligence 316 (Cambridge University Press 2014).

their commitment to ethical values, it is not easy to match this intention with their business purposes whose goals are usually not oriented to public purposes but profit maximisation.

These considerations show why the governance of these technologies is one of the primary challenges that European constitutional law is called to face in the next years. When looking outside the Union, there are different examples of how States are trying to govern the values of the information society by expressing their digital sovereignty to determine the values underpinning the evolution of the tomorrow's digital environment. In the US, the neoliberal approach in the last twenty years would not suggest that the US is expressing its digital sovereignty. The First Amendment has provided a shield against any public interference leading US companies to extend their powers and standards of protection beyond its territory. Nonetheless, even such a liberal approach hides an indirect and omissive way to exercise powers in the digital environment. Rather than intervening in the market, the US has not changed its role and observed its rise as a liberal hub of global tech giants. Regulating online platforms in the US could affect the smooth development of the leading tech companies in the world while also increasing the transparency of the cooperation between the governments and online platforms in certain sectors like security, thus, unveiling the invisible handshake.[44] The Snowden revelations have already underlined how far Governments rely on Internet companies to extend their surveillance programme and escape accountability.[45] Put another way, the US strategy would count on the ability of the private sector to exercise powers on a global scale while benefiting from the invisible cooperation of these actors.

The executive order on preventing online censorship would seem a turning point towards more control online.[46] While, in the last twenty years, nothing has changed in terms of regulating social media on the western side of the Atlantic,[47] now, such a rection would look like just a reminder that States can still impose their sovereignty (and their values) online. The presidential move has resulted in a constitutional paradox.[48] Beyond the constitutional issues involving the separation of powers between the executive and legislative powers, as the former has no power to amend the work of the latter, the order is incoherent when we look at how the First Amendment has protected online intermediaries in the last twenty years.[49] This eventual turning point in the US approach is also surprising when looking at the legislative inertia of the US Congress in the last twenty years.

Likewise, moving from the legislative to judicial power, the order would also be against the recent orientation of the US Supreme Court. Without going into the details of the national case law like *Lewis v YouTube*,[50] we have already underlined in Chapter V how the Supreme Court

[44] Micheal Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Viriginia Journal of Law and Technology 6.
[45] David Lyon, *Surveillance after Snowden* (Polity Press 2015).
[46] Executive Order on Preventing Online Censorship (28 May 2020) <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> accessed 8 June 2020.
[47] See the proposal on The Platform Accountability and Consumer Transparency (PACT) Act (2020) and the
[48] Giovanni De Gregorio and Roxana Radu, 'Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech' MediaLaws (6 June 2020) <http://www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/> accessed 10 June 2020.
[49] Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power Over Online Speech' (2019) Hoover Institution, Aegis Series Paper No. 1902 <https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf> accessed 5 July 2020.
[50] Lewis v YouTube, 197 Cal. Rptr. 3d 219 (Cal. Ct. App. 2015).

defined social media as the vast democratic forum of the Internet in *Packingham v North Carolina*.[51] The order also refers to *Pruneyard Shopping Center v Robins* to argue that, although social media platforms are private actors, they provide a public forum online. Nonetheless, these cases deal with the banning of national law introducing a prior restraint over free speech.[52] These cases should have been enough to impede the public interferences to free speech that this executive order introduces. Besides, in a decision from last year, in *Manhattan Community Access Corp. v Halleck*,[53] the Supreme Court closed the door to a potential extension of the state action doctrine when it decided that private actors, precisely cable tv companies operating public access channels, do not serve as a public actor (i.e. the city of New York) and are thus not bound to protect free speech rights. The relevance of this decision can be understood when looking at the national case law which has already relied on this decision to ban interference with platforms' rights like in *PragerU v YouTube*.[54] Besides, recently, in *Gomez v Zuckenburg*,[55] the Court rejected a user's complaint by recognising that the order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

When looking at China as another technology hub, it is possible to observe a different strategy. China constitutes a paradigmatic example of the opposite path in respect of neoliberal approaches to the digital environment. It has always exercised sovereign powers over the Internet to control online activities.[56] The case of the social credit system is an example of the control that China can exercise in the information society.[57] Such influence has been domestic not only domestic but also international. Together with Russia,[58] China has already tried to dismantle the western multi-stakeholder model by proposing to move internet governance within the framework of the International Telecommunications Union in 2012.[59] In these years, after firstly excluding other digital companies like US tech giants through the Great Firewall,[60] China has created the market to allow its businesses growing outside competition under the Huawei model.[61] This has led to the creation of a Chinese digital political economy. It is true that China is promoting and

[51] Packingham v North Carolina, 582 U.S. ___ (2017).
[52] Pruneyard Shopping Center v Robins, 447 U.S. 74 (1980).
[53] Manhattan Community Access Corp. v. Halleck, No. 17-1702, 587 U.S. ___ (2019).
[54] Prager University v. Google LLC, No. 18-15712 (9th Cir. 2020).
[55] Gomez v Zuckenburg, 2020 U.S. Dist. LEXIS 130989 (N.D.N.Y. July 23, 2020).
[56] Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China' (2003) Harvard Law School Public Law Research Paper No. 62.
[57] Genia Kostka, 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' (2019) 21(7) New Media & Society 1565; Fan Liang and others, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure' (2018) 10(4) Policy & Internet 415.
[58] Eva Claessen, 'Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU' (2020) 5(1) Journal of Cyber Policy 140; Lily H. Newman, 'Russia Takes a Big Step Toward Internet Isolation' Wired (1 May 2020) < https://www.wired.com/story/russia-internet-control-disconnect-censorship/> accessed 4 July 2020.
[59] Julia Bader, 'To Sign or Not to Sign. Hegemony, Global Internet Governance, and the International Telecommunication Regulations' (2019) 15(2) Foreign Policy Analysis 244.
[60] Yu Hong, *Networking China: The Digital Transformation of the Chinese Economy* (University of Illinois Press 2017).
[61] Madison Cartwright, 'Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle' (2020) 9(3) Internet Policy Review <https://policyreview.info/node/1494/pdf> accessed 12 October 2020.

resembling the western conception of the Internet but strongly maintaining control over its businesses. Baidu, Alibaba and Tencent ('BAT'), are increasingly competing with the dominant power of Google, Apple, Facebook, Amazon ('GAFA'). The international success of TikTok is an example of how China aims to attract a global audience of users while supporting its business sector.[62] Put another way, China is only partially opening to digital globalisation while is maintaining control over the network architecture.

The attempts to increase control and create their Internet to increase surveillance and promote their internet economy seems not exhausted. China has shown to have a clear plan for the evolution of the digital environment in the next years. China and its tech giant Huawei have recently proposed a technical shift to the International Telecommunications Union to redesign the TCP/IP protocol and increase centralised control over authentication and communications.[63] Changing the structure of the network is not a neutral choice for the development of the Internet and new digital technologies, including artificial intelligence. This tendency towards centralisation and governance is nothing else that expressing digital sovereignty by reshaping Internet governance and export values outside territorial boundaries through a global channel of communication.[64] The rise of this authoritarian versions of the Internet shows the other side of governance in the algorithmic society.

Within this framework, the Union is going towards a different path. Rather than adopting a mere neoliberal approach or supporting the development of its model of the Internet, it is emerging at the intersection between the two models. The governance of values in the information society is not left either to private determinations through self-regulation or market intervention. The Union is consolidating a co-regulatory approach characterised by the definition of the value framework within which the private sector operates. Therefore, European constitutional values would not just be shaped by private determination or unaccountable forces but protected by a common regulatory framework injecting constitutional values in self-regulation. This result is not by chance but derives from the path of European digital constitutionalism. Despite its capitalistic orientation, as analysed Chapter II, the rise of an increasingly relevant dimension of European constitutional law has mitigated the goals of the internal market and the predominance of self-regulation. The Union's orientation to dignity explains why the rise of private powers is seen as a threat to fundamental rights and democratic values. Unlike the US, the Union's dimension oriented to welfare goals does not allow capitalistic logic to prevail over the social dimension of the European market. This can be understood when looking at the failure of the European model to promote the creation of businesses able to compete with US tech giants. At the same time, the need to ensure competition in the internal market blocks the creation of large corporations while limiting the possibility for Member States' aid to their businesses. Furthermore, the democratic

[62] Michael Keane and Haiqing Yu, 'A Digital Empire in the Making: China's Outbound Digital Platforms' (2019) 13 International Journal of Communication 4624.

[63] Milton Mueller, 'About the Chinese "reinvention" of the Internet… Internet Governance Project blogpost' Internet Governance Project (30 March 2020) <https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/> accessed 1 July 2020.

[64] In countries where extensive forms of surveillance and control over information are diffused, like the Arab States or China, the Internet has repeatedly been subject to public restrictions leading to the blocking of certain online services and/or the strict monitoring of data. See, e.g., Giovanni De Gregorio and Nicole Stremlau, 'Internet Shutdowns and the Limits of Law' (2020) 14 International Journal of Communication 4224.

constitutional basis of the Union precludes any attempt to increase surveillance over the Internet while leaving the doors open to online platforms operating on a transnational scale.

Like in the case of values, the path of European digital constitutionalism would suggest a third way at the intersection between public authority and private ordering. The Union has not shown either its intention to leave the market free to determine the values of the algorithmic society or the interest in intervening in the market to support their business in the rush for becoming a standard maker in the field of artificial intelligence technologies. The Digital Services Act Package and the GDPR provide examples to underline how the Union is struggling to find a proportionate balancing between hard and self-regulation. The Digital Services Act is not just a new legal framework to strengthen the internal market and foster the development of digital services, thus, promoting innovation and new opportunities.[65] Like in the case of the GDPR, it could be considered another way to raise as a global model for regulating transnational powers while protecting democratic values. The two pillars of this package would indeed consist of proposing clear rules for framing digital services responsibilities and ex-ante rules applying to large online platforms acting as gatekeepers, which now set the rules of the game for their users and their competitors.[66] Likewise, the GDPR can be considered a hybrid solution between regulation and self-regulation. As stressed in Chapter VI, the risk-based approach leaves windows of discretion for public and private actors when they implement their data processing. In a certain sense, the Union approach can be considered as an attempt to regulate digital capitalism at the intersection between market logics and democratic values. Put another way, it constitutes a hybrid approach defining that value framework of principles and rules whose boundaries are left to the implementation of transnational businesses under the oversight of judicial power and independent competent authorities.

This approach increasingly tends to promote a governance approach where online platforms are considered regulated centres of collaboration or digital utilities. As underlined in Chapter III, the ability of these actors to govern content and data is not only a risk but also an opportunity to enforce public policies online. The pandemic seasons has fostered this trend where online platforms have shown their predominant role of digital utilities. This situation has underlined the relevance of digital technologies for remote activity and delivery services.[67] We have also seen how, without controlling moderation of content, disinformation and hate speech have spread online. Besides, in the field of data, the example of contact tracing apps is paradigmatic of how Google and Apple have been able to provide a global tracking application, thus, capturing the attention of governments.[68]

---

[65] COM(2020) 37 final (n 2).

[66] See Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services European Commission, Inception impact assessment - Ares(2020)2877686; Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market Inception impact assessment - Ares(2020)2877647.

[67] Daisuke Wakabayashi and others, 'Big Tech Could Emerge from Coronavirus Crisis Stronger Than Ever' The New York Times (23 March 2020) <https://www.nytimes.com/2020/03/23/technology/ coronavirus-facebook-amazon-youtube.html> accessed 5 July 2020.

[68] Oreste Pollicino, 'Contact tracing and COVID-19: Commission and Member States agree on specifications' EU Law Live (16 June 2020) <https://eulawlive.com/contact-tracing-and-covid-19-commission-and-member-states-agree-on-specifications/> accessed 2 July 2020.

Some platforms perform a role beyond the mere provisions of services. While some scholars underlined that their editorial role which should be shielded by the protection of the right to free speech,[69] other scholars underline their role as information or privacy fiduciaries,[70] or as public utilities like infrastructures.[71] The primary point is not opposing their bigness but to regulate their power coming from the governance of social infrastructures. As underlined by Rahman, 'where private actors accumulate outsized control over those goods and services that form the vital foundation or backbone of our political economy—social infrastructure—this control poses dangers'.[72] As underlined by the Council of Europe, '[c]ases where functions traditionally performed by public authorities, such as related to transport or telecommunications, become reliant in full or in part on the provision of algorithmic systems by private parties are also complicated. When such systems are then withdrawn for commercial reasons, the result can range from a decrease in quality and/or efficiency to the loss of services that are considered essential by individuals and communities. States should put contingencies in place to ensure that essential services remain available irrespective of their commercial viability, particularly in circumstances where private sector actors dominate the market in ways that place them in positions of influence or even control'.[73] Within this framework, the concept of public utilities could lead to a solution to find a balanced approach between public authority and private ordering. The increasing control over large parts of political, economic and social life lead online platforms to be critical and essential infrastructures.[74] This dynamic is relevant to the market. The services provided by Google or Facebook play an important role in the success of content creators like traditional media outlets or influencers. The dominance of these actors is not limited to consumer retail sales but also the power over other business sectors relying on their services.

But there is much more beyond economic power. The power of platforms to influence policy-makers and users' behaviours is a dangerous trend for constitutional democracies. This is why the infrastructural nature of these platforms would suggest addressing these challenges through regulating these actors as public utilities. In the US framework, Crawford underlines common carriage concerns would lead to overcoming First Amendment protection without requiring undue speech restraints.[75] Similarly, in the field of search engines, Pasquale underlined the threats

[69] Eric Goldman, 'Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)' Knight First Amendment Institute (February 2018) <https://knightcolumbia.org/content/course-first-amendment- protects-google-and-facebook-and-its-not-close-question> accessed 4 October 2020.
[70] Jack M. Balkin, 'The Fiduciary Model of Privacy' (2020) 134(1) Harvard Law Review Forum; Jack M. Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis Law Review 1183.
[71] K. Sabeel Rahman, 'Monopoly Men' Boston Review (11 October 2017) <http://bostonreview.net/science-nature/k-sabeel-rahman-monopoly-men> accessed 4 October 2020; Cale Guthrie Weissman, 'Maybe It's Time to Treat Facebook Like a Public Utility' Fast Company (1 May 2017) <https://www.fastcompany.com/40414024/maybe-its-time-to-treat-facebook-like-a-public-utility> accessed 4 October 2020; Danah Boyd, 'Facebook Is a Utility; Utilities Get Regulated' Apophenia (15 May 2010) <http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html> accessed 4 October 2020.
[72] K. Sabeel Rahman, 'The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept' (2018) 39 Cardozo Law Review 1621, 1625.
[73] CM/Rec(2020)1 (n 39).
[74] Nikolas Guggenberger, 'Essential Platforms' (2020) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3703361> accessed 9 October 2020.
[75] Susan Crawford, 'First Amendment Common Sense' (2014) 127 Harvard Law Review 2343.

beyond individual privacy including range of biased and discriminatory information results.[76] A framework of public utilities would lead online platforms to perform their business while increasing oversight and fairness. Facebook could be encouraged to ensure more diversity in the organisation of content while Amazon could be required to treat all retailers equally. The idea is not to oppose these social infrastructures which are increasingly critical in daily lives but avoid that their social power overcomes the protection of constitutional values underpinning a democratic society. From services in the market, online platforms have increasingly acquired a foundational or infrastructural role in the information society. Therefore, the power of online platforms coming from the governance of digital infrastructures would deserve a new regulatory framework to protect democratic values in the long run.

This new approach to digital utilities does not mean going back to the end of the last century and adopt a neoliberal perspective based on unaccountable cooperation between the public and private sector. Unlike in the aftermath of the Internet, the Union can rely on a precedent showing the challenges of going back to digital liberalism at the dawn of artificial intelligence technologies. The new phase of digital constitutionalism shows that the Union is aware of this situation. Therefore, the primary challenge for the Union in the algorithmic society is how to ensure that the values underpinning these technologies are not entirely determined by unaccountable private actors but shaped by democratic processes based on transparent and accountable procedures. This would not mean intervening in the market but providing a common regulatory frame of values and principles on which private actors can perform their business. In this case, the Union would follow this path being aware of the challenges of delegating powers to the private sector without ensuring safeguards aimed to protect public values, precisely human dignity.

To ensure that European values at the intersection between digital humanism and capitalism are not left to the determination of private actors, the Union is not taking a hard-regulatory approach which would increase frictions with transnational private actors and potentially undermine individuals' fundamental rights and freedoms. It is indeed proposing a co-regulatory approach as it has been done in the framework of the Digital Single Market Strategy. As underlined by Marsden, co-regulation entails that 'the regulatory regime is made up of a complex interaction of general legislation and a self-regulatory body'.[77] Put another way, the European governance strategy is oriented towards constitutionalising self-regulation.[78] As clarified in the white paper on artificial intelligence, '[i]t is also essential to make sure that the private sector is fully involved in setting the research and innovation agenda and provides the necessary level of co-investment. This requires setting up a broad-based public private partnership, and securing the commitment of the top management of companies'.[79] The Council of Europe has stressed that States should establish appropriate levels of transparency with regard to the public procurement, use, design and basic processing criteria and methods of algorithmic systems implemented by and for them, or by private sector actors. Even more importantly, it underlined that 'the legislative

[76] Frank Pasquale, 'Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines' (2008) University of Chicago Legal Forum 263.
[77] Christopher Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011).
[78] Julia Black, 'Constitutionalising Self-Regulation' (1996) 59 Modern Law Review 24.
[79] COM(2020) 65 final (n 7).

framework for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose'.[80] To face the adverse human rights impacts of artificial intelligence, it is worth working on 'ethics labels or seals for algorithmic systems to enable users to navigate between systems',[81] while ensuring 'particularly high standards as regards the explainability of processes and outputs'.[82]

Co-regulation implemented through different system like public-private partnership or public utilities regulation would be the third way that digital constitutionalism would promote in the European framework. Between granting a pressive regulation of the digital environment and leaving the private sector to establish the predominant values, the Union is defining a constitutional framework where it provides the general values which then should be implemented by the private sector. In this way, online platforms would not operate as governors of fundamental rights online but as regulated entities driven by a mix of profit maximisation and public purposes. The focus of the Council of Europe on the introduction of algorithmic impact assessment is an evident example of the European way to increase the accountability of the public and private sector when implementing artificial intelligence technologies.[83] As observed by the Council of Europe, '[p]rivate sector actors engaged in the design, development, sale, deployment, implementation and servicing of algorithmic systems, whether in the public or private sphere, must exercise due diligence in respect of human rights. […] This responsibility exists independently of States' ability or willingness to fulfil their human rights obligations. As part of fulfilling this responsibility, private sector actors should take continuing, proactive and reactive steps to ensure that they do not cause or contribute to human rights abuses and that their actions, including their innovative processes, respect human rights. They should also be mindful of their responsibility towards society and the values of democratic society'.[84]

Considering the global reach and dissemination of algorithmic technologies, this framework will increasingly underline the role of the Union as a global regulator. Put another way, rather than governing or neglecting market dynamics, the Union is tailoring its role in between. Nonetheless, being a global regulator would clash with traditional territorial limits to the exercise of sovereign powers. Even if the Union is proposing its approach to algorithmic technologies on a global scale, still the hybrid approach between hard and self-regulation meets some limits. Therefore, the next subsection addresses the third dilemma focusing on whether digital constitutionalism would increase the tendency towards extraterritoriality of European values or, instead, promote a phase of constitutional protectionism to avoid external interferences undermining fundamental rights and democratic values.

4. Scope: Constitutional Imperialism v Constitutional Protectionism

The global nature of these challenges leads to focusing on how far European digital constitutionalism could extend its influence to protect fundamental rights and democratic values in the algorithmic society. If, on the one hand, the Union has shown to be oriented towards the

[80] CM/Rec(2020)1 (n 39).
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Ibid.

sustainable development of algorithmic technologies and adopt a hybrid governance strategy between public values and private ordering, being a global regulator entails dealing with the external limits of sovereign powers. Territory is the natural limitation of States' sovereign power. Inside a certain territory, citizens are expected to comply with the applicable law in that area while, outside this framework, they would be subject to the influence of other sovereign powers. As stressed in Chapter III, the Internet, as an expression of globalisation, has challenged the traditional model to exercise sovereign powers. At the same time, the potential global reach of new technologies does not necessarily leave States unarmed against overseas interferences. The cases of China or Russia show how these countries are proposing alternatives for governing digital technologies which tend to reflect their values.[85] Therefore, in order to understand the evolution of European digital constitutionalism in the algorithmic society, it is worth wondering whether the Union would focus on extending powers to protect constitutional values beyond its territorial boundaries (i.e. constitutional imperialism) or follow an opposite phase towards limiting its influence just to the European territory (i.e. constitutional protectionism).

The Union has already shown its ability to influence global dynamics, so that scholars have named such attitude as the 'Brussel effect'.[86] The Union is increasingly aware of its ability to extend its 'regulatory soft power', influencing the policy of other areas of the world in the field of new technologies. It has also started to build its narrative about digital sovereignty.[87] As underlined by the Commission, 'European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks and communications' aimed to mitigate 'dependency on other parts of the globe for the most crucial technologies'.[88] This does not entail closing European boundaries towards a form of constitutional protectionism but to ensure the Union's ability to define its rules and values in the digital age. Indeed, 'European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model',[89] and, as a result, 'the EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based'.[90] These statements would suggest that Union is taking its path towards a leading role in regulating the digital environment and artificial intelligence technologies. Rather than focusing just on promoting the European industry, the Union approach is oriented towards rising as a global standard maker. Its narrative is not adversarial but cooperative.

The GDPR is one example of the tendency of the Union to act as a global regulator.[91] The

[85] Dennis Broeders and others, 'Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' The Hague Program for Cyber Norms Policy Brief (November 2019) < https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace> accessed 5 July 2020.
[86] Anu Bradford, *The Brussels Effect. How the European Union Rules the World* (Oxford University Press 2020). See also Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2018) 62 American Journal of Comparative Law 87.
[87] COM(2020) 67 final (n 5), 2.
[88] Ibid, 2.
[89] Ibid.
[90] Ibid.
[91] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L 119/1.

European framework of data protection has raised as a model for other legislation in the world,[92] so that UN Secretary General has welcomed the European approach by underlining how this measure is inspiring for other countries and encouraged the Union and its Member States to follow this path.[93] Furthermore, the adoption of the GDPR has led a growing number of companies to voluntary comply with some of the rights and safeguards even for data subjects outside the territory of the Union because protecting privacy and personal data has become a matter of reputation due to the increasing amount of data processed by public and private actors.[94] The recent spread of the pandemic has shown the relevance of data protection safeguards' for constitutional democracies when dealing with contact tracing applications or other forms of public surveillance.[95]

Besides, the GDPR has not only become a model at the global level but also provide a scope of application which would extend beyond the European territory. Precisely, even though the data controller is established outside the European Union, European data protection law is nevertheless applicable if the activities of which the processing of personal data implies the provision of products or services to data subjects who are in the Union and (ii) the processing activities are related either to the a) offering of goods and services in the EU; or b) to the monitoring of the behaviour of data subjects in the EU.[96] By extending the scope of application of the GDPR, the Union would seem to adopt a form of constitutional imperialism by imposing its own legal standard of protection on a global scale.

Nonetheless, while it is true that the GDPR is rising as a global model for the protection of privacy and personal data, it is not driven by a mere goal of extraterritoriality or imperialism. Rather, it shows that the Union aims to ensure that formal territorial limitations would not undermine the protection of fundamental rights of privacy and data protection and the related democratic values in the Union. The extraterritorial reach of European data protection law and, in general of the GDPR can be considered an 'anti-circumvention mechanism'.[97] The ECJ has contributed to explaining the need to extend European rules to ensure the effective protection of fundamental rights. The GDPR territorial scope of application has codified the doctrine of establishment developed by the ECJ in *Weltimmo* and *Google Spain*.[98] In *Weltimmo*, the ECJ adopted a broad interpretation of the concept of 'establishment' avoiding any formalistic approach linked to the place of companies' registration. Likewise, in *Google Spain*, the ECJ underlined this flexible interpretation '[i]n the light of the objective pursued by Directive 95/46, consisting in

[92] Graham Greenleaf, Global Data Privacy Laws 2019: 132 National Laws & Many Bills (2019) 157 Privacy Laws & Business International Report 14.
[93] Address of the UN Secretary-General to the Italian Senate, 18 December 2019 <https://www.un.org/press/en/2019/sgsm19916.doc.htm> accessed 3 July 2020.
[94] Cisco, 'Consumer Privacy Study. The Growing Imperative of Getting Data Privacy Right (November 2019) <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf> accessed 2 July 2020.
[95] Oreste Pollicino, 'Fighting COVID-19 and Protecting Privacy under EU Law. A Proposal Looking at the Roots of European Constitutionalism' EU Law Live (16 May 2020) <https://eulawlive.com/weekend-edition/weekend-edition-no17/> accessed 4 October 2020.
[96] GDPR (n 91), Art 3(2).
[97] Svetlana Yakovleva, and Kristina Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation' (2020) 114 AJIL Unbound 10.
[98] Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság (2015); Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014).

ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data'.[99] 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's case-law, since even those entities that are not established in the Union will be subject to the GDPR. On the other hand, the primary consequence of such an extension of territoriality is to extend European constitutional values to the global context.

The European influence as a global regulator also leads other legal systems to adapt their standards of protection to ensure an essentially equivalent degree of protection with European safeguards. The ECJ confirmed this extensive trend in the *Schrems* case,[100] by invalidating the Commission's adequacy decision,[101] known as the 'safe harbour agreement', concerning the transfer of personal data from the Union to the US. In this case, it is possible to observe another manipulation of data protection law extending its boundaries across the Atlantic. Although the Data Protection Directive required US data protection law to ensure an 'adequate' level of protection,[102] the ECJ went beyond this boundary by stating that the safeguards should be 'equivalent' to those granted by EU law to ensure the effective protection of the fundamental rights to privacy and data protection as enshrined in the Charter.[103]

However, this decision did not exhaust the concerns about the safeguards in the transfer of personal data across the Atlantic. The ECJ invalidated the new adequacy decisions (i.e. Privacy Shield),[104] in light of the protection of fundamental rights as also translated into the new framework for personal data transfer introduced by the GDPR.[105] The ECJ went even further assessing the Standard Contractual Clauses ('SCCs') framework. Even without invalidating the Commission Decision on the use of these clauses,[106] the ECJ underlined that the equivalent level of protection applies even to this legal instrument. The court expressly underlined the limits of EU law in relation to third countries since SSCs are not capable of binding the authorities of that third country.[107] Therefore, the ECJ recognised the role of the controller established in the Union and the recipient of personal data to check and monitor whether the third country involved ensures

[99] C-131/12 (n 98).
[100] Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015). See Oreste Pollicino and 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 The Global Community Yearbook of International Law and Jurisprudence 2016, 245.
[101] 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.
[102] 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, Art 25.
[103] C-362/14 (n 100).
[104] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016) OJ L 207/1.
[105] C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (2020).
[106] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010) OJ L 39/5.
[107] ibid, 136.

an essentially equivalent degree of protection.[108] When this is not the case, the ECJ did not preclude the transfer but underlined the need to set additional safeguard to ensure that degree of protection.[109] This system has recognised the freedom of business actors to define the standard of protection of personal data across the Atlantic. Besides, Daskal underlined the limits of the entire system since 'there is no guarantee that the companies will win such challenges; they are, after all, ultimately bound by U.S. legal obligations to disclose. And even more importantly, there is absolutely nothing that companies can do to provide the kind of back-end judicial review that the Court demands'.[110]

The long arm of European data protection law has been already highlighted in the framework ofthe Data Protection Directive,[111] the 'global reach of EU law'.[112] It cannot be excluded that this over-reaching scope could affect free speech and financial interests of other countries and their citizens,[113] and decrease the degree of legal certainty leading to a binary approach which is not scalable.[114] The GDPR has also been criticised for its 'privacy universalism'. [115] Proposing the GDPR as a global model entails exporting a western conception of privacy and data protection that could clash with the values of other areas of the world, especially, the global south. Although other scholars do not share the same concerns, they have observed that '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'.[116]

The ECJ has recently highlighted these 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.[117] Within this framework, the ECJ ruled on a preliminary reference concerning the territorial scope of the right to be forgotten online. The case initially arose from a formal notice which the President of the CNIL submitted to Google requiring the search engine to delist information of data subjects from all its domain name extensions. Google refused to comply with such a request arguing that the removal of links in the

[108] ibid, 135, 137, 142.
[109] ibid, 133.
[110] Jennifer Daskal, 'What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers' Just Security (17 July 2020) <https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/> accessed 29 July 2020.
[111] 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?' (2011) 1(1) International Data Privacy Law 28.
[112] Christopher Kuner, 'The Internet and the Global Reach of EU Law', in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019).
[113] Dan J.B. Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3(4) International Data Privacy Law 278, 1.
[114] Christoper Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235; Svantesson (n 113).
[115] Payal Arora, 'GDPR – A Global Standard? Privacy Futures, Digital Activism and Surveillance Cultures in the Global South' (2019) 17(5) Surveillance & Society 717.
[116] Paul de Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6(3) International Data Privacy Law 230, 240.
[117] Case C-507/17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (2019).

case in question could just concern the results from the domain names of its search engine in the Member States. Google also proposed the application of geo-blocking measures according to which users would have been prevented from accessing the results from an IP address deemed to be located in the State of residence of a data subject, no matter which version of the search engine they used. The French Court asked whether the delisting performed by a search engine should be global or limited to the domain name of the State in which the request is deemed to have been made or to the national extensions of all Member States, including the possibility to apply geo-blocking techniques in this last case.

As initial steps, the ECJ firstly clarified that, although the Data Protection Directive was in force on the date of the request for the preliminary ruling, this legal instrument was repealed by the GDPR. Therefore, the court took into consideration both measures to allow national courts to rely on an applicable interpretation. Secondly, the Luxembourg judges recalled the interpretation of the *Google Spain* decision concerning the role of fundamental rights of privacy and data protection in defining the scope of the right to the delist based on Articles 12(b) and 14(1)(a) of the Data Protection Directive,[118] and the notion of establishment based on the assessment of the context of activities involving the processing of personal data regardless of whether that processing takes place in the Union.[119] Based on these assumptions, the ECJ observed that the scope of the Data Protection Directive and the GDPR is to guarantee a high level of protection of personal data within the Union and, therefore, a de-referencing covering all the domains of a search engine (i.e. global delisting) would meet this objective. This is because the role of search engines in disseminating information is relevant on a global scale since users can access links to information 'regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself'.[120]

Nevertheless, the ECJ underlined the limits of this global approach. Firstly, States around the world do not recognise the right to delist or provide different rules concerning the right to be forgotten online.[121] Even more importantly, since the right to privacy and data protection are not absolute rights, they need to be balanced with other fundamental rights,[122] among which the right to freedom of expression.[123] The protection of these fundamental rights (and, therefore, their balance) is not homogenous around the world. The GDPR does not aim to strike a fair balance between fundamental rights outside the territory of the Union.[124] Before this crossroads, rather than extending the boundaries of data protection law to the global scale, the ECJ followed the opinion of the AG Szpunar,[125] thus, observing that neither the Data Protection Directive nor the GDPR recognises the right of data subjects to require a search engine like Google to delist content worldwide.[126] Therefore, although Google falls under the scope of European data protection law, it is not required to delist information outside the territory of Member States. Nonetheless,

[118] C-131/12 (n 98), 88, 99.
[119] Ibid, 56-60.
[120] C-507/17 (n 117), 57.
[121] Ibid, 58.
[122] Ibid, 59.
[123] See Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (2010), 48; Opinion 1/15 EU-Canada PNR Agreement (2017), 136.
[124] GDPR (n 91) Art 17(3)(a).
[125] Opinion of Advocate General in Google Inc. v Commission nationale de l'informatique et des libertés (10 January 2019), 63.
[126] C-507/17 (n 117), 64.

Member States still maintain the possibility to issue global delisting order according to their legal framework. The ECJ specified that, if, on the one hand, EU law does not require search engines to remove links and information globally, on the other hand, it does not ban this practice. It is for Member States to decide whether extending the territorial scope of judicial and administrative order according to their constitutional framework of protection of privacy and personal data balanced with the right to freedom of expression.[127]

The ECJ also explained that the impossibility to require search engines to delist information on a global scale is the result of the lack of cooperation instruments and mechanisms in the field of data protection. The GDPR only provides the supervisory authorities of the Member States with internal instruments of cooperation to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data against the interest of the public in various Member States in having access to information.[128] Therefore, such instruments of cooperation cannot be applied outside the territory of the Union.

Regarding the second question concerning the territorial scope of delisting within the territory of the Union, the ECJ observed that the adoption of the GDPR aims to ensure a consistent and high level of protection of personal data in all the territory of the Union and, therefore, delisting should be carried out in respect of the domain names of all Member States.[129] Nonetheless, the ECJ acknowledged that, even within the Union, the interest of accessing information could change between Member States as also shown the degree of freedom Member States enjoy in defining the boundaries of processing in the field of freedom of expression and information pursuant to Article 85 of the GDPR.[130] In other words, the ECJ underlined not only that freedom of expression does not enjoy the same degree of protection at the international level but also, in Europe, it can vary from one Member State to another. Therefore, it is not possible to provide a general obligation to delist links and information applying to all Member States.

To answer this issue, the court left this decision to national supervisory authorities which through the system of cooperation established by the GDRP should, *inter alia*, reach 'a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union'.[131] Likewise, even concerning geo-blocking techniques, the ECJ did not interfere with Member States' assessment about these measures just recalling by analogy that 'these measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name'.[132] By distancing itself from the AG Szpunar's view on this point,[133] the ECJ decided not to recognise a general removal obligation at the European level but relied on the mechanism of cooperation of national authorities as well as to the discretion of Member States concerning preventing measures.

---

[127] Case C-617/10, Åklagaren v Hans Åkerberg Fransson (2013), 29; C-399/11, Stefano Melloni v Ministerio Fiscal (2013), 60.
[128] GDPR (n 91), Arts 56, 60-66.
[129] C-507/17 (n 117), 66.
[130] Ibid, 67.
[131] Ibid, 68.
[132] Ibid, 70. See, *inter alia,* Case C-484/14, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (2016), 96.
[133] Opinion of Advocate General in C-507/17 (n 125), 78.

Just one week later, in *Glawischnig-Piesczek v Facebook*,[134] the court addressed the territorial extension of national injunctions concerning the removal of content. The ECJ observed that Article 18 of the e-Commerce Directive does not provide for any limitation to the territorial scope of the measures that Member States can adopt and, consequently, EU law does not prevent a national order to extend the scope application of their measures globally. As a general limit, the ECJ specified that Member States should take into consideration their international obligations given the global dimension of the circulation of content, without either specifying which rules of international law would apply in this case.

With regard to the territorial extension of national order, the ECJ did not clarify to which rules of international law the Member States should refer to assess the territorial scope of removal orders. Some perspectives on this point can be found in the decision *Google v CNIL*. In this case, the ECJ expressly refers to the potential contrast of a global delisting order with the protection of rights at an international level. Therefore, competent national authorities can indeed strike a fair balance between individuals' right to privacy and data protection with the right to freedom of information. However, the different protection of freedom of expression at a global level would limit the application of the balancing results. The AG Szpunar reaches the same conclusion in the Facebook case, explaining that, although EU law leaves Member States free to extend the territorial scope of their injunctions outside the territory of the Union, national courts should limit their powers to comply with the principle of international comity.[135]

This trend towards local removal is based not only on the *status quo* of EU law at the time of the decisions but also on the effects that a general extension of global remove can produce in the field of content and data. As observed by the AG Szpunar, a worldwide de-referencing obligation could initiate a 'race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale'.[136] In other words, the ECJ's legitimacy could start a process of cross-fertilisation, thus, leading other countries to extend their removal order on a global scale. This could be particularly problematic when looking at authoritarian countries which could exploit this decision to extend their orders.[137]

Moreover, in *Google v CNIL*, the ECJ explained that the limit for global removal also comes from the lack of intention to confer an extraterritorial scope to right to erasure established by the GDPR.[138] The lack of cooperation mechanisms between competent authorities extending outside the territory of the Union would confirm this argument. Nevertheless, by supporting this position, the ECJ did not consider that, more generally, the GDPR establishes a broad territorial of application covering processing activities related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.[139]

---

[134] Case C-18/18, *Eva Glawischnig-Piesczek* v Facebook (2019).
[135] Opinion of Advocate General in Eva Glawischnig-Piesczek v Facebook Ireland Limited (4 June 2019), 100.
[136] Ibid, 61.
[137] Dan B. J. Svantesson, 'Bad News for the Internet as Europe's Top Court Opens the Door for Global Content Blocking Orders' Linkedin (3 October 2019) <https://www.linkedin.com/pulse/bad-news-internet-europes-top-court-opens-door-global-svantesson/> accessed 12 May 2020.
[138] C-507/17 (n 117), 62.
[139] GDPR (n 91), Art 3(2).

Nonetheless, it is worth underlining that the Union has not closed the doors to the possibility of extending the territorial scope of removal orders beyond EU borders. At first glance, the ECJ seems to express at an opposite view in the two cases regarding the territorial scope of national orders. On the one hand, in *Google v CNIL*, the ECJ stated that EU law does not require search engines to carry out the delisting of information and links on a global scale. In *Glawischnig-Piesczek v Facebook*, on the other hand, the ECJ explained that there are no obstacles to global removal, but also it leaves the evaluation to the Member States. Although the two judgments may seem opposite, they lead to the same result, namely that EU law does not either impose or preclude national measures whose scope extends worldwide. This is a decision which rests with Member States which are competent to assess their compliance with international obligations. Art. 18 of the e-Commerce Directive does not provide a specific territorial scope of application and the ECJ has not gone further. Otherwise, 'it would have trespassed within the competencies of Member States, which under EU law retain primary legislative power on criminal law matters'.[140] Besides, the reasons for this different approach can be attributed to the different degree of harmonisation of the protection of personal data and defamation as observed by the AG Szpunar.[141] Therefore, it is not just an issue concerning public international law but also private international law contribute to influencing the territorial scope of removal orders.[142]

Despite the relevance of the aforementioned point, leaving Member States free to determine when a national order should be applied globally could lead to different national approaches which would fragment harmonisation goals. This is particularly relevant in the framework of the GDPR since it provides a new common framework for Member States in the field of data. Indeed, while the content framework still relies on the e-Commerce Directive leaving margins of discretion to Member States, this approach in the field of data is more problematic. On the one hand, the GDPR extends its scope of application to ensure a high degree of protection of fundamental rights of the data subjects. On the other hand, such a framework can be questioned by the autonomy of Member States to decide the reach of the right to be forgotten online. As Zalnieriute explains, '[b]y creating the potential for national data protection authorities to apply stronger protections than those afforded by the GDPR, this decision could be seen as another brick in the "data privacy wall" which the CJEU has built to protect EU citizens'.[143]

Furthermore, even in this case, the ECJ has not focused on the peculiarities of platforms' activities and the consequences of these decisions on the governance of freedom of expression in the digital space. In *Glawischnig-Piesczek v Facebook*, a local removal order would not eliminate the possibility of accessing the same content – identical or equivalent – through the use of other technological systems or outside the geographical boundaries envisaged by the removal order. This problem is particularly relevant in *Google v CNIL* since it is possible to access different Google domain names around the world easily. The interest in the protection of reputation could also require an extension beyond the borders of the Union to avoid relying just on partial or

[140] Elda Brogi and Marta Maroni, 'Eva Glawischnig-Piesczek v Facebook Ireland Limited: A New Layer of Neutrality' CMPF (7 October 2010) <https://cmpf.eui.eu/eva-glawischnig-piesczek-v-facebook-ireland-limited-a-new-layer-of-neutrality/> accessed 19 May 2020.
[141] Opinion Advocate General in C-18/18 (n 135), 79.
[142] Paolo Cavaliere, 'Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations' (2019) 4 European Data Protection Law 573, 577.
[143] Monika Zalnieriute, 'Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)' (2020) 114(2) American Journal of International Law 261.

ineffective remedies. The ECJ recognised that access to the referencing of a link referring to information regarding a person in the EU is likely to have 'immediate and substantial effects on the person'.[144] Therefore, even if this statement is just one side of the balancing activity with the protection of international law on the other side, it leads to contradictory results frustrating data subjects' right to be forgotten due to the potential access to search engines' domain names. Furthermore, to comply with geographical limits, geo-blocking and other technical measures would require an additional effort for platforms, thus, increasing the risk of censorship on a global scale and create a technological barrier for small-medium platforms.

It is possible to observe how one of the consequences of this political choice of the Union is to increase the regulatory burdens for those entities which, although not established in the EU territory, offer of goods and services or monitor the behaviour of data subjects in the Union. In other words, the Union is trying to ensure that formal geography could not constitute a shield to avoid compliance with any regulation. Rather than a European data privacy imperialism, this approach would aim to protect users' fundamental rights,[145] while avoiding that businesses escape from complying with EU law just by virtue of a formal criterion of establishment. Otherwise, the primary risk is to encourage a disproportionate unbalance between businesses operating physically in the territory of a State, and other entities which, by processing data and offering other digital services, would avoid complying with the law of the States in which perform their business.

Therefore, the extraterritorial effects of European data protection law would not express a form of constitutional imperialism or protectionism. The need to ensure the protection of fundamental rights in a globalised world leads the Union to exercise a global influence which, at first glance, would be the opposite of constitutional protectionism. At the same time, the Union is aware of the consequences of the extension of constitutional values on the global scale which, according to the ECJ case law, seems to appear an exceptional resort based on Member States' assessment. In this way, the Union is rising as global regulator proposing a political model to transnationally to limit interferences oppressive models of governance based on wide liberal approach or oppressive public control. In other words, rather than adopting an extraterritorial or protectionist approach, the Union seems to have chosen a third way once again. Like in the case of values and governance, the Union has shown its intent to take a third way proposing its role as a global regulator rather than a liberal or authoritarian hub for tech giants. In this way, European constitutional standard would not only promote the sustainable development of artificial intelligence in the long term but also, in the short term, limit and mitigate the competitive advantage of other States.

Such a third way is the result of the role of European digital constitutionalism which, in these years, has shown how rights and freedoms cannot be frustrated just by formal doctrines based on territory and establishment. At the same time, European digital constitutionalism does not look to have imperialist goals but rather propose a political and normative model to protect fundamental rights and democratic values on a global scale.

[144] C-507/17 (n 117), 57.
[145] de Hert and Czerniawski (n 116).

5. Conclusions: The Constitutional Lesson Learnt and the Digital Road Ahead

The rise of digital constitutionalism has shown to what extent the shift from atoms to bits has affected the constitutional rules and values underpinning the social contract. The evolution of the Internet and new automated decision-making technologies has provided invaluable opportunities for the exercise of fundamental rights and democratic values while unveiling the opaque side of a new system of values and governance of a global society whose values are still rooted and fragmented in local constitutional traditions. We have examined how the talent of European constitutional law has provided a first reaction to the challenges of the information society.

The answer to the first research question, 'what are the reasons for the rise of European digital constitutionalism?', has led to focus on the reaction of the Union to challenges of the information society. In these years, the digital environment, as an expression of globalisation, has met local dynamics and values. It led to questioning how the traditional notion of sovereignty and power does not entirely fit within transnational forms of power. Global phenomena like migrations, the environment and digital technologies challenge the traditional exercise of public powers which are traditionally linked to a certain territory and population. The traditional notion of the law, as expression of States' authority, seems increasingly nuanced and competing with norms (auto)produced by other subsystems. The unitary of State and its law is slowly replaced by the fragmentation of new institutions expressing their principles and values on a global scale. Put another way, from 'law and territory', we increasingly are moving to the relevance of the relationship between 'norms and space'. Non-state actors, private corporations, and supranational governance institutions contributes to defining their rules and code of conducts whose global reach overlaps with the traditional expression of national sovereign power. This should come as a surprise. It is the inevitable result of globalisation leading to an intertwined scenario made of norms and values at the global level. Such a parallel production of standards and norms for the digital environment inevitably meet local constitutional values. States rely on the possibility to express sovereign powers enjoying the exclusive monopoly on the use of force. International organisations and global organisations develop standards for the digital environment, while transnational private actors, precisely online platforms, privately determine the boundaries to moderate content and process data, thus, rising as social infrastructure. In this process of mutual influence between global and local dynamics, constitutional values are just a small piece of jigsaw.

Before the constitutionalisation of global subsystems, the Union has entered into a new digital constitutional phase. In Chapter II, we have seen how, from a neoliberal opening to the digital environment at the end of the last century, the European approach has turned into a constitutional strategy. This process has not been casual but constitutional-driven. At the end of the last century, the Union adopted a digital liberal approach oriented to trust in the ability of the internal market to grow thanks to new digital products and services. The fear to overwhelm the market and slow the development of this promising technological framework governed the European approach at the end of the last century. The strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were going to revolutionise the entire society and promising new opportunities. The minimum harmonisation adopted in the field of content and data can be considered two examples of the neoliberal approach characterising the first phase of the Union's approach to the digital environment.

The end of this phase was the result of two events which, at the very least, have led to the end of the first (liberal) season and trigger a new phase of the European path characterised by the role of the ECJ in paving the way towards digital constitutionalism through judicial activism. Precisely, the emergence of the Nice Charter as a bill of rights and the increasing relevance of globalised dynamics and the consolidation of private powers in the digital environment have played a critical role to move the perspective of the Union from economic freedoms to fundamental rights and democratic values. The rise of digital constitutionalism in Europe has been characterised by two primary characteristics. Firstly, the codification of the ECJ's efforts to extend the protection of fundamental rights in the digital environment has translated judicial activism into a regulatory outcome. Secondly, within the framework of the Digital Single Market strategy, the Union has also clarified its intention to limit platforms' powers by fostering the degree of transparency accountability of online platforms and asking these actors to protect core values. This phase of European digital constitutionalism has shown the talent of European constitutional law to provide a first reaction not only against public interferences but also the exercise of digital powers by transnational private actors.

Nonetheless, the reaction of European digital constitutionalism to the challenges of the information society is not enough to explain the characteristics of digital powers. This is because the second question of this work focused on answering 'what are the characteristics and the limits of platforms' powers in the digital environment?'. As examined in Chapter III, the liberal approach adopted at the end of the last century has empowered online intermediaries to enforce public policies online. Requiring online intermediaries to remove 'illegal' content based on their awareness is an example of delegation to the private sector of functions traditionally vested in public authorities, namely the definition of content legality. Public safeguards like due process have not been translated in the private sector, thus, leaving online platforms to set their own procedure to moderate content and process personal data on a global scale. In this way, platforms have been free to remove content or block account without any accountability, no matter if they affect speech on a global scale. The same is in the field of data where the risk-based approach leaves data controllers margins of discretion in defining the degree of safeguard which would meet their accountability in a certain context while relying on a legal framework which, although considering consent as the basic pillar of users' autonomy, it leaves data controllers to rely on other legal bases to achieve their purposes.

The lack of safeguards mixed to the opportunities of new processing technologies has led these actors to complement delegated with autonomous powers. Such a new form of (digital) power is also the result of the capability to extract value from the processing of data and organisation of content through the implementation of artificial intelligence technologies. The private development of digital and automated decision-making technologies has not only challenged the protection of individuals' fundamental rights such as freedom of expression and data protection. This new technological framework has also empowered online platforms to perform quasi-public functions in the transnational context. It is because of these technologies if the freedom to conduct business has turned into power. Focusing just on the delegation of powers would not provide a clear picture of the power which online platforms exercise when discretionarily setting and enforcing rules driven by private determinations rather than constitutional values. Online platforms vertically order the relationship with users' while autonomously setting the rules to

enforce and balance users' fundamental rights by using automated decision-making processes without any constitutional safeguard.

These considerations are still not enough to explain the characteristics of digital powers in the information society. Another critical piece of the constitutional puzzle is at the intersection of the legal regimes of content and data. As examined in Chapter IV, it is possible to understand the consolidation of platforms' powers by looking at the blurring boundaries of the legal regimes of expression and data in the algorithmic society which, in the phase of digital liberalism, have been conceived on parallel tracks. This choice, which could seem neutral at the end of the last century when online intermediaries performed passive activities, is now questioned by a digital environment made of active providers whose business model is based on the extraction of value.

When looking at online platforms, precisely social media and search engines, it is possible to understand the technological intersection between the legal regimes of content and data. These actors operate as data controllers when deciding the means and the purposes of processing personal data while they can also be considered processors for the data they host. On the other hand, platforms actively organise content according to the data they collect from users even if they can rely on an exemption of liability for hosting and organising third-party illicit content. The mix of content and data liability's regimes makes easier for online platforms to shield their activities in the blurring lines between the two regimes. The organisation of users' content and the processing of data are part of a unique framework even if the legal regimes of content and data have been conceived on parallel tracks. In other words, the technological divergence between content and data at the end of the last century has converged towards overlapping layers of protection.

This situation leads to wonder whether European digital constitutionalism could provide a normative solution. In order to unveil the normative side of this phase, the third question of this research aims to examine: 'which remedies European constitutional law can provide to solve the imbalances of power in the algorithmic society and mitigate the risks for fundamental rights and democratic values?' The reaction of digital constitutionalism has been just a first step. The talent of European constitutional law is not just to react against the rise of digital powers but also propose a normative framework for protecting democratic values in the long run. Still, the primary issues in the field of content and data led to thinking about the role of European constitutional law to address the primary challenges for fundamental rights and democracy in the algorithmic society.

As underlined in Chapter V, protecting freedom of expression just as a liberty cannot be enough to ensure an effective protection of this fundamental right in the algorithmic society. The process of content moderation has shown how online platforms, as private actors, exercise their powers on freedom of expression on a global scale while maintaining their immunity. Despite the step forward made within the framework of the Digital Single Market strategy, users cannot still rely on a clear set of transparency and accountability safeguards in the process of content moderation. Users do not usually know the criteria or the logic on which their expressions are organised and filtered or even removed. The lack of any safeguard and remedy against online platforms' discretion in moderating content leads to thinking about the instruments that constitutional law can provide to remedy this situation. While, in the lack of regulation, the horizontal application of freedom of expression could not be a general solution but just a reactive approach, rethinking media pluralism online could be another view to rely on the States'

obligations to ensure not the only the negative but also positive side of freedom of expression. European constitutional law could promote a uniform regulatory framework of the procedures to moderate content. Such a normative approach would not aim to dismantle the system of platforms' liability nor regulate speech. Instead, it consists of limiting platforms discretion and introducing procedural safeguards in content moderation, precisely in the phases of notice, decision-making and redress.

When moving to the field of data, the normative side of European digital constitutionalism looks slightly different. As analysed in Chapter VI, the reactive approach of digital constitutionalism has not been enough to address the challenges of the algorithmic society to privacy and data protection. Unlike in the case of content, individuals can rely on a positive framework of safeguards which aim to mitigate private powers through instruments of transparency and accountability. The GDPR is a paradigmatic example of this approach. Nonetheless, this does not mean that digital constitutionalism has achieved its purpose. The GDPR leaves broad margins of discretion by adopting a risk-based approach where the data controller becomes the arbiter of personal data protection. For this reason, to avoid that such freedom turns into forms of power, the normative side of European digital constitutionalism in the field of data consists of providing constitutional guidance. The GDPR includes values underpinning European constitutionalism. Precisely, the principles of human dignity, proportionality and due process are the core driving values of European data protection law. These values can provide the normative interpretation on which lawmakers and courts can rely to scrutinise and mitigate data controllers' discretion, thus, maintaining their accountability without overwhelming the private sector with further obligations.

The talent of European constitutional law to react and propose a normative framework to remedy the exercise of digital powers is only a starting point before the challenges of the algorithmic society. The fourth research question was oriented to understand: 'which paths the consolidation of European digital constitutionalism could open to the Union in the next years?' The previous sections of this chapter have underlined how digital constitutionalism could find its 'third way' to address the challenges of the algorithmic society. In front of the regulatory crossroad in the field of artificial intelligence, the Union seems to have chosen a path towards the development of a sustainable artificial intelligence environment rather than focusing just on fostering innovation to exploit the potentialities of these technologies or merely impeding their development to protect fundamental rights and democratic values. Likewise, in order to limit autonomous determinations of public values by the private sector, the Union is rising as a global regulator whose approach is based on co-regulation. The challenges raised by self-regulation and the risk of hard regulation have led the Union to choose a third way even in this case by proposing a hybrid system of governance based on a common framework of public values guiding the determinations of the private sector. The scope of this system of governance is another tile of the mosaic. The need to protect fundamental rights and democratic values from global challenges has not led the Union to enter into a phase of constitutional imperialism or protectionism. It has raised a balanced approach which limits the extraterritoriality of European constitutional values while avoiding that formal justifications substantially undermine the protection of fundamental rights and democratic values.

These challenges have led the Union to learn an important constitutional lesson. Neoliberal approaches without public safeguards would clash with the characteristics of European

constitutionalism. Fundamental rights and democratic values cannot be left in the hands of unaccountable actors developing technologies which promise to provide new opportunities for growth while moving decisions affecting daily lives outside democratic circuits. Against the threats coming from ubiquitous automation putting aside the role of humans, European digital constitutionalism can rely on a set of safeguards and guarantees among which human dignity play a critical role as constitutional guidance. These characteristics would reveal the mission of European digital constitutionalism: rising like a shield against the discretionary exercise of private powers putting human under a new *status subjectionis* driven by the logics of digital capitalism. European constitutionalism protects dignity even when humans do not meet the expectation of a capitalist system to protect them from its consequences like poverty and inequality. Within this framework, European digital constitutionalism would constitute a shield against processes of dehumanisation driven by digital capitalism. Even if it could be difficult to compare to the experience of the last century, the rise of private powers could fragment the path European constitutionalism has taken so far.

A fourth phase or a more mature expression of digital constitutionalism would aim to oppose to techno-determinist solutions and contribute to promoting European values as a sustainable constitutional model for the development of automated technologies on the global context. Therefore, the primary goal of digital constitutionalism in the algorithmic society would be to promote and safeguard constitutional values from the rise of digital powers. The road ahead of digital constitutionalism is far from being straight, but the path already made so far seems to be promising.

Bibliography

- Abrams F., *The Soul of the First Amendment* (Yale University Press 2017).
- Ackerman B., *We The People: Transformations* (Belknap Press 1998).
- Alexy R., *A Theory of Constitutional Rights* (Oxford University Press 2002).
- Alexy R., A Theory of Rights (Oxford University Press 1985).
- Ali M. and others, 'Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes' in *Proceedings of the ACM on Human-Computer Interaction* (ACM 2019).
- Allegri M.R. and d'Ippolito G. (eds), *Accesso a Internet e neutralità della Rete, tra principi costituzionali e regole europee* (Aracne 2017).
- Allgood B., 'The Commoditization of AI and The Long-Term Value of Data' Forbes (10 April 2017) https://www.forbes.com/sites/forbestechcouncil/2017/04/10/the-commoditization-of-ai-and-the-long-term-value-of-data/#74c71abd159c.
- Alpa G., Bessone M. and Boneschi L. (eds), *Il diritto all'identità personale* (Cedam 1981).
- Alpa G., 'Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto all'identità personale' (1989) (2) Giurisprudenza di merito 464.
- Alter A., *Irresistible: The Rise of Addictive Technology and the Business of Keeping us Hooked* (Penguin Press 2017).
- Amato G. and Paciotti E. (eds), *Verso l'Europa dei diritti. Lo Spazio europeo di liberta, sicurezza e giustizia* (Il Mulino 2005).
- Ammori M., 'The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter' (2014) 127 Harvard Law Review 2259.
- Araya D., 'Governing The Fourth Industrial Revolution' Forbes (12 May 2019) https://www.forbes.com/sites/danielaraya/2019/03/12/governing-the-fourth-industrialrevolution/#4eea13a14b33.
- Ardia D.S., 'Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act' (2010) 43 Loyola of Los Angeles Law Review 373.
- Arendt H., *The Human Condition* (University of Chicago Press 1998).
- Arora P., 'GDPR – A Global Standard? Privacy Futures, Digital Activism and Surveillance Cultures in the Global South' (2019) 17(5) Surveillance & Society 717.
- Article 19, 'The Social Media Councils: Consultation Paper' (2019) https://www.article19.org/wp- content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf.
- Augenstein D. and Dziedzic L., 'State Responsibilities to Regulate and Adjudicate Corporate Activities under the European Convention on Human Rights' (2017) EUI Working papers https://cadmus.eui.eu/bitstream/handle/ 1814/48326/LAW_2017_15.pdf?sequence=1&isAllowed=y.
- Auletta T., *Riservatezza e tutela della personalità* (Giuffrè 1978).
- Ausloos J., *The Right to Erasure in EU Data Protection Law* (Oxford University Press 2020).
- Azzariti G., 'Internet e Costituzione' (2011) (3) Politica del diritto 367.
- Bader J., 'To Sign or Not to Sign. Hegemony, Global Internet Governance, and the International Telecommunication Regulations' (2019) 15(2) Foreign Policy Analysis 244.
- Bagger Tranberg C., 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 International Data Privacy Law 239.

- Baldassarre A., 'Il diritto di privacy e la comunicazione elettronica' (2010) (1) Percorsi costituzionali 49.
- Baldassarre A., *Privacy e Costituzione: l'esperienza statunitense* (Bulzoni Editore 1974).
- Balkin J.M., 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 New York University Law Review 1.
- Balkin J.M., 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 University of California Davis 1151.
- Balkin J.M., 'Free Speech and Hostile Environments' (1999) 99 Columbia Law Review 2295.
- Balkin J.M., 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis Law Review 1183.
- Balkin J.M., 'Old-School/New-School Speech Regulation' (2014) 128 Harvard Law Review 2296.
- Balkin J.M., 'The Fiduciary Model of Privacy' (2020) 134(1) Harvard Law Review Forum.
- Balkin J.M., 'The Future of Free Expression in a Digital Age' (2009) 36 Pepperdine Law Review 427.
- Barak A., Proportionality Constitutional Rights and their Limitations (Cambridge University Press 2012).
- Barata J., '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.
- Barendt E., 'Balancing Freedom of Expression and Privacy' (2009) 1(1) Journal of Media Law 49.
- Barendt E., *Freedom of Speech* (Oxford University Press 2017).
- Barile P., *Liberta di manifestazione del pensiero* (Giuffrè 1975).
- Barkan J., 'Law and the Geographic Analysis of Economic Globalization' (2011) 35(5) Progress in Human Geography 589.
- Barlow J.P., 'A Declaration of Independence of the Cyberspace' (Electronic Frontier Foundation 1996) www.eff.org/cyberspace-independence.
- Barlow J.P., 'The Economy of Ideas: Selling Wine Without Bottles on the Global Net' in Peter Ludlow (ed), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (MIT Press 1999).
- Barocas S. and others, 'Governing Algorithms: A Provocation Piece', SSRN (4 April 2013) https://ssrn.com/abstract=2245322.
- Barocas S. and Selbst A.D., 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
- Barocas S., Hood S. and Ziewitz M., 'Governing Algorithms: A Provocation Piece' (2013) https://ssrn.com/abstract=2245322.
- Caryn Devins and others, 'The Law and Big Data' (2017) 27 Cornell Journal of Law and Public Policy 357.
- Barrett P.M., 'Who Moderates the Social Media Giants? A Call to End Outsourcing' NYU Centre for Business and Human Rights (June 2020) https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/5ed9854bf618c710cb55be9/1591313740497/NYU+Content+Moderation+Report_June+8+2020.pdf.
- Barron P. and Morrison S., 'Pluralism after scarcity: the benefits of digital technologies' LSE Media Policy Project blog (18 November 2014) http://blogs.lse.ac.uk/mediapolicyproject/2014/11/18/ pluralism-after-scarcity-the-benefits-of-digital-technologies/.

- Barzilai-Nahon K., 'Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control' (2008) 59(9) Journal of the American Society for Information Science and Technology 1493.
- Bassini M. and Vigevani G.E., 'Primi appunti su fake news e dintorni' (2017) (1) Rivista di diritto dei media 11.
- Bassini M., 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) 25(2) European Law Journal 182.
- Bassini M., 'La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità 'complessa'?' (2015) Federalismi.it https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=30349.
- Bassini M., 'Mambo Italiano: the Italian perilous way on ISP liability' in Tuomas Ojanen and Byliana Petkova (eds), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries* (forthcoming, Edward Elgar).
- Bassini M., *Internet e Libertà di Espressione. Prospettive Costituzionali e Sovranazionali* (Aracne 2019).
- Bathaee Y., 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology 890.
- Bayer J. and Carrera S., 'A Comparative Analysis of Media Freedom and Pluralism in the EU Member States' (2016) Study for the LIBE Committee http://www.europarl.europa.eu/RegData/etudes/ STUD/2016/571376/IPOL _STU(2016)571376_ EN.pdf.
- Beijer M., *The limits of Fundamental Rights Protection by the EU: The Scope for the Development of Positive Obligations* (Intersentia 2017).
- Bell E. and Owen T., 'The Platform Press: How Silicon Valley Reengineered Journalism' Tow Centre for Digital Journalism (29 March 2017) https://www. cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php.
- Belli L. (ed.), *Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking, and Traffic Management* (FGV Direito Rio 2016).
- Belli L. and Venturini J., 'Private Ordering and the Rise of Terms of Service as Cyber-Regulation' (2016) 5(4) Internet Policy Review (2016) https://policyreview.info/node/441/pdf.
- Belli L., Francisco P.A. and Zingales N., 'Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police' in Luca Belli and Nicolo Zingales (eds), *How Platforms are Regulated and How They Regulate Us* 41 (FGV Rio 2017).
- Ben-Shahar O. and Schneider C.E., *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2016).
- Benjamin S.M., 'Algorithms and Speech' (2013) 161(4) University of Pennsylvania Law Review 1446.
- Benkler Y., 'Degrees of Freedom Dimension and Power' (2016) 145 Daedalus 18.
- Benkler Y., *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006).
- Bennett Moses L., 'How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target' (2013) 5(1) Law, Innovation and Technology 1.
- Berman P.S., 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 University of Colorado Law Review 1263.
- Betzu M., 'Anonimato e responsabilità in internet' (2016) costituzionalismo.it https://www.costituzionalismo.it/ anonimato-e-responsabilita-in-internet/.
- Betzu M., *Regolare Internet. Libertà di informazione e di comunicazione nell'era digitale* (Giappichelli 2012).

- Bianca C.M., *Le autorita private* (Jovene 1977).
- Bickert M., 'Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process, Facebook' (24 April 2018) https://newsroom.fb.com/news/2018/04/comprehensive-community-standards.
- Binns R. and others, 'Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation' in Giovanni L. Ciampaglia, Afra Mashhadi and Taha Yasseri. *Social Informatics* (Springer 2017).
- Binns R., 'Data Protection Impact Assessment: A Meta-Regulatory Approach' (2017) 7(1) International Data Privacy Law 22.
- Birnhack M. and Elkin-Koren N., 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Viriginia Journal of Law and Technology 6.
- Black J., 'Constitutionalising Self-Regulation' (1996) 59(1) The Modern Law Review 24.
- Bloch-Webba H., 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU Law Review 27.
- Blocher J., 'Institutions in the Marketplace of Ideas' (2008) 57(4) Duke Law Journal 820.
- Boehme-Neßler V., 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection' (2016) 6(3) International Data Privacy Law 222.
- Bognetti G., *La libertà d'espressione nella giurisprudenza americana. Contributo allo studio dei processi dell'interpretazione giuridica* (Istituto Editoriale Cisalpino 1958).
- Bognetti G., 'The Concept of Human Dignity in U.S. and European Constitutionalism' in Georg Nolte (ed.), *European and US Constitutionalism* (Cambridge University Press 2005).
- Bognetti G., *Lo spirito del costituzionalismo americano: breve profilo del diritto costituzionale degli Stati Uniti* (Giappichelli 2000).
- Bollinger L.C. and Stone G.R. (eds), *The Free Speech Century* (Oxford University Press 2019).
- Bond S., 'Google and Facebook Build Digital Duopoly' Financial Times (14 March 2017) ft.com/content/30c81d12-08c8-11e7-97d1- 5e720a26771b.
- Borejsza J.W. and Ziemer K. (eds), *Totalitarian and Authoritarian Regimes in Europe: Legacies and Lessons from the Twentieth Century* (Berghahn 2007).
- Bostrom N. and Yudkowsky E., 'The Ethics of Artificial Intelligence' in Keith Frankish and William M. Ramsey (eds), The Cambridge Handbook of Artificial Intelligence (Cambridge University Press 2014).
- Boyd D. and Crawford K., 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2015) 15 Information Communication and Society 662.
- Boyd D., 'Facebook Is a Utility; Utilities Get Regulated' Apophenia (15 May 2010) http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.
- Boyle J., 'A Nondelegation Doctrine for the Digital Age?' (2000) 50 Duke Law Journal 5.
- Boyle J, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' (1997) 66 University of Cincinnati Law Review 177.
- Bozdag E., 'Bias in Algorithmic Filtering and Personalization' 15(3) Ethics and Information Technology 209.
- Bradford A., *The Brussels Effect. How the European Union Rules the World* (Oxford University Press 2020).
- Brand P. and Getzler J. (eds), *Judges and Judging in the History of the Common Law and Civil Law: From Antiquity to Modern Times* (Cambridge University Press 2015).

- Brandeis L.D., 'The Curse of Bigness', in Osmond K. Fraenkel (ed), *The Curse of Bigness: Miscellaneous Papers of Louis D. Brandeis* (Viking Press 1934).
- Brauneis R. and Goodman E.P., Algorithmic Transparency for the Smart City (2018) 20 Yale Journal of Law and Technology 103.
- Brey P.A.E. and Soraker J., *Philosophy of Computing and Information Technology* (Elsevier 2009).
- Bridy A., 'Remediating Social Media: A Layer-Conscious Approach' (2018) 24 Boston University Journal of Science & Technology Law 193.
- Brietzke P.H., 'How and Why the Marketplace of Ideas Fails' (1997) 31(3) Valparaiso University Law Review 951.
- Bryson J., 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation' in Markus D. Dubber, Frank Pasquale, and Sunit Das (eds), *The Oxford Handbook on Ethics of AI* (Oxford University Press 2020).
- Brkan M., 'Freedom of Expression and Artificial Intelligence: On Personalisation, Disinformation and (Lack Of) Horizontal Effect of the Charter' SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_ id=3354180.
- Broeders D. and others, 'Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' The Hague Program for Cyber Norms Policy Brief (November 2019) https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace.
- Brogi E. and Maroni M., 'Eva Glawischnig-Piesczek v Facebook Ireland Limited: A New Layer of Neutrality' CMPF (7 October 2010) https://cmpf.eui.eu/eva-glawischnig-piesczek-v-facebook-ireland-limited-a-new-layer-of-neutrality/.
- Brown I. and Marsden C., *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013).
- Brownsword R. and Yeung K. (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008).
- Bucher T., 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook' (2012) 14(7) New Media & Society 1164.
- Burrell J., 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society 1.
- Burris S., Drahos P. and Shearing C., 'Nodal governance' (2005) 30 Australian Journal of Legal Philosophy 30.
- Busch C. and others, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 5 Journal of European Consumer and Market Law 3
- Bygrave L.A., *Internet Governance by Contract* (Oxford University Press 2015)
- Califano L., 'Principi e contenuti del Regolamento 2016/679/UE in materia di protezione dei dati personali' in Lucia Scaffardi (ed), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale* (Giappichelli 2018).
- Calo R., 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 UC Davis Law Review 399.
- Cantwell Smit B., *The Promise of Artificial Intelligence. Reckoning and Judgment* (MIT Press 2019).
- Cartabia M., 'Europe and Rights: Taking Dialogue Seriously' (2009) 5(1) European Constitutional Law Review 5.
- Cartabia M., 'I diritti fondamentali in Europa dopo Lisbona. Verso nuovi equilibri?' (2010) (3) Giornale di diritto amministrativo 221.
- Cartwright M., 'Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle' (2020) 9(3) Internet Policy Review https://policyreview.info/node/1494/pdf.

- Caretti P., 'Art. 10 – Liberta di espressione' in Sergio Bartole, Benedetto Conforti and Guido Raimondi (eds), *Commentario alla convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali* 337 (Cedam 2001).
- Caruso C., *La libertà di espressione in azione. Contributo a una teoria costituzionale del discorso pubblico* (Bononia University Press 2013).
- Casey B., Farhangi A. and Vogl R., 'Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' (2019) 34 Berkeley Technology Law Journal 143.
- Casonato C., 'Intelligenza artificiale e diritto costituzionale: prime considerazioni' (2019) Diritto Pubblico Comparato ed Europeo 101.
- Cassano G. and Cimino I.P., 'Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"? Un primo commento agli artt. 14 -17 del d.lgs. 70/2003' (2004) (3) Giurisprudenza italiana 671.
- Castells M., *Networks of Outrage and Hope: Social Movements in the Internet Age* (Polity Press 2012).
- Cavaliere P., 'Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations' (2019) 4 European Data Protection Law 573.
- Celeste E., 'Digital Constitutionalism: A New Systematic Theorization' (2019) 33(1) International Review of Law, Computers and Technology 76.
- Celeste E., 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2018) International Review of Law, Computers and Technology https://www.tandfonline.com/doi/abs/10.1080/13600869.2018.1475898.
- Chander A. and Le U.P., 'Data Nationalism' (2015) 64(3) Emory Law Journal 677.
- Chander A., 'Facebookistan' (2012) 90 North Carolina Law Review 1807.
- Chen A. 'The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed' Wired (23 October 2014) https://www.wired.com/2014/10/content-moderation/.
- Chenou J.M. and Radu R., 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2017) 58 Business & Society 74.
- Christou G., and Simpson S., 'The Internet and Public–Private Governance in the European Union' (2006) 26(1) Journal of Public Policy 43.
- Cisco, 'Consumer Privacy Study. The Growing Imperative of Getting Data Privacy Right (November 2019) https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf.
- Citron D.K. and Norton H.L., 'Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age' (2011) 91 Boston University Law Review 1436
- Citron D.K. and Pasquale F., 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1.
- Citron D.K. and Wittes B., 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity' (2017) 86 Fordham Law Review 401.
- Citron D.K., 'Technological Due Process' (2008) 85 Washington University Law Review 1249.
- Claessen E., 'Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU' (2020) 5(1) Journal of Cyber Policy 140.
- Clark J. and others, 'The Shifting Landscape of Global Internet Censorship' (2017) Berkman Klein Center for Internet & Society Research Publication https://dash.harvard.edu/handle/1/33084425.
- Clegg N., 'Welcoming the Oversight Board' Facebook (6 May 2020) https://about.fb.com/news/ 2020/05/welcoming-the-oversight-board/.

- Coase R., 'Markets for Goods and Market for Ideas' (1974) 64(2) American Economic Review 1974.
- Cobbe J. and Bietti E., 'Rethinking Digital Platforms for the Post-COVID-19 Era' CIGI (12 May 2020) https://www.cigionline.org/articles/rethinking-digital-platforms-post-covid-19-era.
- Coeckelbergh M., *AI Ethics* (MIT Press 2020).
- Cohen J., 'Intellectual Privacy and Censorship of the Internet' (1998) 8(3) Seton Hall Constitutional Law Journal 693.
- Cohen J., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
- Cohen J.E., 'What Privacy Is For' (2013) 126 Harvard Law Review 1904.
- Cohen J.E., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
- Cohen M.R., 'Property and Sovereignty' (1927) 13 Cornell Law Review 8.
- Costanzo P., 'Aspetti evolutivi del regime giuridico di Internet' (1996) (6) Diritto dell'Informazione e dell'informatica 831.
- Costanzo P., 'Il fattore tecnologico e le sue conseguenze' (2012) (4) Rassegna parlamentare 811.
- Costanzo P., 'Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)' (2012) Consulta Online http://www.giurcost.org/studi/Costanzo15.pdf.
- Craig P., 'EU Accession to the ECHR: Competence, Procedure and Substance' (2013) 35 Fordham International Law Journal 111.
- Crawford K. and Gillespie T., 'What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint' (2016) 18 New Media & Society 410.
- Crawford K. and Schultz J., 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 Boston College Law Review 93
- Crawford S., 'First Amendment Common Sense' (2014) 127 Harvard Law Review 2343.
- Crisafulli V., 'Problematica della "libertà di informazione"' (1964) 29(2) Il Politico 285.
- Cumbley R. and Church P., 'Is Big Data Creepy?' (2013) 29 Computer Law and Security Review 601.
- Cuniberti M., 'Democrazie, dissenso politico e tutela dell'anonimato' (2014) (2) Diritto dell'informazione e dell'informatica 111.
- Cuniberti M., 'Il contrasto alla disinformazione in rete' (2017) (1) Rivista di diritto dei media 26.
- Custers B. and others (eds), *Discrimination and Privacy in the Information Society* (Springer 2013).
- D'Acquisto G. and Others, 'Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics', ENISA (December 2015) https://www.enisa.europa.eu/publications/big-data-protection.
- D'Arcus B., 'Extraordinary Rendition, Law and the Spatial Architecture of Rights' (2014) 13 ACME: An International E-Journal for Critical Geographies 79.
- Dainow J., 'The Civil Law and the Common Law: Some Points of Comparison' (1966-1967) 15(3) American Journal of Comparative 419.
- Daly A., *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016).
- Danaher J., 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 Philosophy & Technology 245.
- Daskal J., 'What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers' Just Security (17 July 2020) https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/.

- De Burca G. and Aschenbrenner J.B., 'The Development of European Constitutionalism and the Role of the EU Charter of Fundamental Rights' (2003) 9 Columbia Journal of European Law 355.
- De Burca G., 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20(2) Maastricht Journal of European and Comparative Law 168.
- De Burca G., 'The Road Not Taken: The EU as a Global Human Rights Actor' (2011) 105(4) American Journal of International Law 649.
- De Cata M., *La responsabilità civile dell'*internet service provider (Giuffrè 2010).
- De Cupis A., *Il diritto all'onore e il diritto alla riservatezza* (Giuffrè 1948).
- De Gregorio G. and Radu R., 'Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech' MediaLaws (6 June 2020) <http://www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/> accessed 10 June 2020.
- De Gregorio G. and Stremlau N., 'Internet Shutdowns and the Limits of Law' (2020) 14 International Journal of Communication 4224.
- De Gregorio G., 'From Constitutional Freedoms to Powers: Protecting Fundamental Rights Online in the Algorithmic Society' (2019) 11(2) European Journal of Legal Studies 65.
- de Hert P. and Czerniawski M., 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6(3) International Data Privacy Law 230.
- de Hert P. and Gutwirth S., 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* 3 (Springer 2009).
- de Hert P. and Kloza D., 'Internet (Access) as a new Fundamental Right. Inflating the Current Rights Framework?' (2012) 3(2) European Journal of Law and Technology http://www.ejlt.org/index.php/ejlt/article/view/123/268
- de Hert P. and others, 'The Right to Data Portability in GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34(2) Computer Law & Security Review 193.
- de Hert P., 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in David Wright and Paul de Hert (eds), *Privacy Impact Assessment* 33 (Springer 2012)
- de Hert P., 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Patrizio Campisi, *Security and Privacy in Biometrics* 369 (Springer 2013)
- de Hing A., 'Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation' (2018) 19(5) German Law Journal 1270
- De Minico G., *Internet. Regola e anarchia* (Jovene 2012).
- De Secondat C., *L'esprit des loi* (1748).
- De Witte B. and Imanovic S., 'Opinion 2/13 on Accession to the ECHR: Defending the EU Legal Order against a Foreign Human Rights Court' (2015) 5 European Law Review 683.
- Deibert R. and others, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008).
- Delaney D. 'Legal Geography I: Constitutivities, Complexities, and Contingencies' (1996) 39(1) Progress in Human Geographies 96.
- Delfini F., 'La responsabilità dei prestatori intermediari nella direttiva 2000/13/CE e nel d.lgs. 70/2003' (2004) (1) Rivista di diritto privato 55.
- Della Cananea G., *Due Process of Law Beyond the State: Requirements of Administrative Procedure* (Oxford University Press 2016).

- Della Morte G., *Big data e protezione internazionale dei diritti umani. Regole e contenuti* (Editoriale Scientifica 2018).
- Devins C. and others, 'The Law and Big Data' (2017) 27 Cornell Journal of Law & Public Policy 357.
- DeVito M.A., 'From Editors to Algorithms' (2017) 5(6) Digital Journalism 753.
- Di Ciommo F., 'Programmi-filtro e criteri di imputazione/ esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down' (2010) (6) Diritto dell'informazione e dell'informatica 829.
- Di Lello C., 'Internet e Costituzione: garanzia del mezzo e suoi limiti' (2007) (4-5) Diritto dell'informazione e dell'informatica 895.
- Diakopoulos N., 'Algorithmic Accountability. Journalistic Investigation of Computational Power Structures' (2014) 3 Digital Journalism 398.
- Dignum V., *Responsible Artificial Intelligence* (Springer 2019).
- Dinwoodie G.B. (ed.), *Secondary Liability of Internet Service Providers* (Springer 2017).
- Donati F., 'Art. 11 – Libertà di espressione e di informazione' in Raffaele Bifulco, Marta Cartabia and Alfonso Celotto (eds*), L'Europa dei diritti – Commento alla Carta dei diritti fondamentali dell'Unione europea* 100 (Il Mulino 2001).
- Douek E., 'Facebook's "Oversight Board:" Move Fast with Stable Infrastructure and Humility' (2019) 21(1) North Carolina Journal of Law & Technology 1.
- Douglas-Scott S., 'A Tale of Two Courts: Luxembourg, Strasbourg and the Growing European Human Rights Acquis' (2006) 43 Common Market Law Review 629.
- Douglas-Scott S., 'The European Union and Human Rights after the Treaty of Lisbon' (2011) 11(4) Human Rights Law Review 645.
- Douglas-Scott S., 'The Relationship between the EU and the ECHR Five Years on from the Treaty of Lisbon' in Sybe De Vries, Ulf Bernitz and Stephen Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing* 41 (Hart 2015)
- Dreyer S. and Schulz W., 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole', (2019) Bertelsmann Stiftung https://www.bertelsmann-stiftung.de/doi/10.11586/2018018.
- Duprè C., *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Hart 2015).
- Dworkin R., *Freedom's Law: The Moral Reading of the American Constitution* (Oxford University Press 1999).
- Dwoskin E. & Tiku N., 'Facebook Sent Home Thousands of Human Moderators due to the Coronavirus. Now the Algorithms are in Charge' The Washington Post (24 March 2020) https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/.
- Dylko I. and others, 'The Dark Side of Technology: An Experimental Investigation of the Influence of Customizability Technology on Online Political Selective Exposure' (2017) 73 Computers in Human Behavior 181.
- Easterbrook F.H., 'Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Forum 207.
- Edwards L. and Veale M., 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.
- Edwards L., 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 1 European Data Protection Law 26.
- Edwards L., 'The Problem of Intermediary Service Provider Liability' in Lilian Edwards (ed), *The New Legal Framework for E-Commerce in Europe* 93 (Hart 2005).

- Eichensehr K.E., 'Digital Switzerlands' (2018) 167 University Pennsylvania Law Review 665.
- El Emam K. and A´ lvarez A., 'A Critical Appraisal of the Article Working Party Opinion 05/2014 on Data Anonymization Techniques' (2015) 5 International Data Privacy Law 73.
- Elkin-Koren N. and Haber E., 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2017) 82(1) Brooklyn Law Review 105.
- Elkin-Koren N. and Perel M., 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed.), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).
- Erdos D., 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection' (2015) 52 Common Market Law Review 119.
- Erdos D., 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' (2018) 26 International Journal of Law and Information Technology 189.
- Eskens S. and others, 'Challenged by News Personalisation: Five Perspectives on the Right to Receive Information (2017) 9(2) Journal of Media Law 259.
- Esposito C., *La libertà di manifestazione del pensiero nell'ordinamento italiano* (Giuffrè 1958).
- European Centre for Press and Media Freedom, 'Promoting Dialogue Between the European Court of Human Rights and the Media Freedom Community. Freedom of Expression and the Role and Case Law of the European Court of Human Rights: Developments and Challenges' (2017) https://www.ecpmf.eu/archive/files/ecpmf-ecthr_conference_e-book.pdf.
- Evans D.S., 'Governing Bad Behavior by Users of Multi-Sided Platforms' (2012) 27 Berkeley Technology Law Journal 1201.
- Fabbrini F., 'The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal 65-
- Favaretto M., De Clercq E. and Elger B.S., 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 Journal of Big Data 12.
- Feeley M., 'EU Internet Regulation Policy: The Rise of Self-Regulation' (1999) 22(1) Boston College International and Comparative Law Review 159.
- Ferrajoli L., *Diritti fondamentali. Un dibattito teorico* (Laterza 2001).
- Ferrarese M.R., *Le istituzioni della globalizzazione. Diritto e diritti nella societa' transnazionale* (Il Mulino 2000).
- Ferrarese M.R., *Prima Lezione di diritto globale* (Laterza 2012).
- Ferri G.B., 'Diritto all'informazione e diritto all'oblio' (1990) Rivista diritto civile 801.
- Festinger L., *A Theory of Cognitive Dissonance* (Stanford University Press 1957).
- Fichera M., *The Foundations of the EU as a Polity* (Edward Elgar 2018).
- Finck M. and Pallas F., 'They who Must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10(1) International Data Privacy Law 11.
- Finocchiaro G., 'La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "Schrems"' (2015) (4-5) Diritto dell'informazione e dell'informatica 779.
- Finocchiaro G., 'Riflessioni sul rapporto tra diritto e tecnica' (2012) (4-5) Diritto dell'informazione e dell'informatica 831.
- Fisher M., 'Inside Facebook's Secret Rulebook for Global Political Speech' New York Times (27 December 2018) https://www.nytimes.com/2018/12/27/world/facebook-moderators.html.

- Fitzgerald B., 'Software as Discourse - A Constitutionalism for Information Society' (1999) 24 Alternative Legal Journal 144.
- Fleishmandec G., 'Cartoon Captures Spirit of the Internet' The New York Times (14 December 2000) https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html.
- Fletcher R. and Nielsen R.K., 'Are News Audiences Increasingly Fragmented? A Cross-National Comparative Analysis of Cross-Platform News Audience Fragmentation and Duplication' (2017) 67(4) Journal of Communication 476.
- Flew T. and others, 'Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance' (2019) 10(1) Journal of Digital Media & Policy 33.
- Floridi L. (ed.), *The Onlife Manifesto Being Human in a Hyperconnected Era* (Springer 2015).
- Floridi L. and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28(4) Minds and Machines 689.
- Floridi L., 'AI and Its New Winter: From Myths to Realities' (2020) 33 Philosophy & Technology 1.
- Floridi L., 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307.
- Floridi L., 'The Green and the Blue: Naïve Ideas to Improve Politics in a Mature Information Society' in Carl Öhman and David Watson, *The 2018 Yearbook of the Digital Ethics Lab* 183 (Springer 2018).
- Floridi L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).
- Foer F., 'Facebook's war on free will' The Guardian (19 September 2017) https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will.
- Fois S., 'Questioni sul fondamento costituzionale del diritto alla "identità personale"' in Guido Alpa and others (eds), *L'informazione e i diritti della persona* 159 (Jovene 1983).
- Fois S., *Principi costituzionali e libera manifestazione del pensiero* (Giuffrè 1957).
- Forgó N. and others, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales and Others (eds), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation* 17 (Springer 2017).
- Franklin M., *Digital Dilemmas: Power, Resistance, and the Internet* (Oxford University Press 2013).
- Frantziou E., 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (2015) 21(5) European Law Journal 657.
- Frantziou E., *The Horizontal Effect of Fundamental Rights in the European Union A Constitutional Analysis* (Oxford University Press 2019).
- Fraser N., 'Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy' (1990) 25/26 Social Text 56.
- Freeman J. and Minow M. (eds), *Government by Contract Outsourcing and American Democracy* (Harvard University Press 2009).
- Fried C., 'Privacy: A Moral Analysis' (1968) 77 Yale Law Journal 475.
- Froomkin A.M., 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461.
- Froomkin A.M., 'The Internet as a Source of Regulatory Arbitrage' in Brian Kahin and Charles Nesson (eds), *Borders in Cyberspace* 129 (MIT Press 1997).
- Froomkin A.M., 'Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution' (2000) 50 Duke Law Journal 17.
- Frosini T.E., 'Internet come ordinamento giuridico' (2014) (1) Percorsi costituzionali 13.

- Frosini T.E., 'Tecnologie e libertà costituzionali' (2003) (3) Diritto dell'informazione e dell'informatica 487.
- Frosini V., 'Il diritto alla riservatezza' in Vittorio Frosini, *Il diritto nella società tecnologica* (Giuffrè 1981).
- Frosini V., 'L'orizzonte giuridico dell'internet' (2000) (2) Diritto dell'Informazione e dell'informatica 270.
- Frosini V., *Il diritto tra potere e liberta nell'era tecnologica*, in Vittorio Frosini, *Il giurista e le tecnologie dell'informazione* (Bulzoni Editore 1998).
- Frosini V., *La protezione della riservatezza nella società informatica* (1981) (1) Informatica e diritto 5.
- Frosio G., 'The Death of "No Monitoring Obligations": A Story of Untameable Monsters' (2017) 8(3) Journal of Intellectual Property, Information Technology 212.
- Frosio G. and Mendis S., 'Monitoring and Filtering: European Reform or Global Trend?' in Giancarlo Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability* 544 (Oxford University Press 2020).
- Gabrielli E. (ed), *Il diritto all'oblio* (Editoriale scientifiche 1999).
- Gal M.S. and Aviv O., 'The Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349.
- Gal M.S. and Aviv O., 'The Unintended Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349.
- Galgano F., *La globalizzazione nello specchio del diritto* (Il Mulino 2005).
- Gardbaum S., 'Proportionality and Democratic Constitutionalism' in Grant Huscroft and others (eds), *Proportionality and the Rule of Law. Rights, Justification, Reasoning* 259 (Cambridge University Press 2014).
- Gardbaum S., 'The Horizontal Effect of Constitutional Rights' (2003) 102 Michigan Law Review 388.
- Gates B., *The Road Ahead* (Viking Press 1995).
- Geiger S., 'Does Habermas Understand the Internet? The Algorithmic Construction of the Blogo/Public Sphere' (2009) 10(1) Gnovis: A Journal of Communication, Culture, And Technology http://www.gnovisjournal.org/2009/12/22/does-habermas-understand-internet-algorithmic-construction-blogopublic-sphere/.
- Gellert R., 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279.
- Gellert R., *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).
- Geradin D., 'What Should EU Competition Policy do to Address the Concerns Raised by the Digital Platforms' Market Power?' (2018) TILEC Discussion Paper No. 2018-041 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3011188.
- Geradin D., Katsifis D. and Karanikioti T., 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech' (2020) TILEC Discussion Paper No. 2020-012 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130.
- Gillespie T., *Custodians of The Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).
- Gillespie T., 'Regulation of and by Platforms' in Jean Burgess, Alice E. Marwick and Thomas Poell (eds), *The SAGE Handbook of Social Media* 254 (Sage 2018).
- Gillespie T., 'The Politics of Platforms' (2010) 12(3) News Media & Society 347.
- Gillespie T., 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (eds) *Media Technologies Essays on Communication, Materiality, and Society* 167 (Oxford University Press 2014).
- Gillis T.B. and Spiess J.L., 'Big Data and Discrimination' (2019) 86 The University of Chicago Law Review 459.

- Ginsburg T. and Simpser A. (eds), *Constitutions in Authoritarian Regimes* (Cambridge University Press 2014).
- Ginsburg T., Huq A.Z. and Versteeg M., 'The Coming Demise of Liberal Constitutionalism?' (2018) 85(2) The University of Chicago Law Review 239.
- Gitlan T., 'Public Sphere or Public Sphericules?' in Tamar Liebes and James Curran (eds), *Media, Ritual and Identity* 168 (Routledge 2002).
- Goel V., 'Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry' The New York Times (29 June 2014) https://www.nytimes.com/2014/06/30/technology /facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.
- Goldman A.I. and Cox J.C., *Speech, Truth, and the Free Market for Ideas* (Cambridge University Press 1996).
- Goldman E., 'Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)' Knight First Amendment Institute (February 2018) https://knightcolumbia.org/ content/course-first-amendment-protects-google-and-facebook-and-its-not-close-question.
- Goldsmith J. and Wu T., *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)
- Goldsmith J.L., 'The Internet and the Abiding Significance of Territorial Sovereignty' (1998) 5 Indiana Journal of Global Legal Studies 474
- Goldsmith J.L., 'The Internet, Conflicts of Regulation and International Harmonization', in Christoph Engel (ed.), *Governance of Global Networks in the Light of Differing Local Values* 197 (Nomos 2000).
- Goldsmith J.L., 'Against Cyberanarchy' (1999) 40 University of Chicago Law Occasional Paper 1
- Gonzalez Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).
- Goodman B. and Flaxman S., 'EU Regulations on Algorithmic Decision-Making and a "Right To Explanation"' (2016) 83 AI magazine 3.
- Goodman B. and Flaxman S., 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 AI Magazine 50.
- Gorwa R., Binns R. and Katzenbach C., 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) Big Data & Society https://journals.sagepub.com/doi/pdf/10.1177/2053951719897945.
- Graber C.B., 'Bottom-Up Constitutionalism: The Case of Net Neutrality' (2017) 7 Transnational Legal Theory 524.
- Graef I., *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility: Data as Essential Facility* (Wolter Kluwer 2016).
- Graells A. S., *Public Procurement and the EU Competition Rules* (Hart 2015).
- Greenleaf G., 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 2(2) University of New South Wales Law Journal 593.
- Greenleaf G., 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 Privacy Laws & Business International Report 14.
- Gregg A. and Greene J., 'Pentagon awards controversial $10 billion cloud computing deal to Microsoft, spurning Amazon' Washington Post (26 October 2019) https://www.washingtonpost.com/business/2019/10/25/pentagon-awards-controversial-billion-cloud-computing-deal-microsoft-spurning-amazon/.
- Grimmelmann J., 'Speech Engines' (2014) 98 Michigan Law Review 868;
- Grimmelmann J., 'The Virtues of Moderation' (2015) 17 Yale Journal of Law and Technology 42.

- Grimmelmann J., 'Virtual World Feudalism' (2009) 118 Yale Law Journal Pocket Part 126.
- Grygiel J. and Brown N., 'Are Social Media Companies Motivated to Be Good Corporate Citizens? Examination of the Connection Between Corporate Social Responsibility and Social Media Safety' (2019) 43 Telecommunications Policy 445
- Gualco E. and Lourenço L. '"Clash of Titans". General Principles of EU Law: Balancing and Horizontal Direct Effect' (2016) 1(2) European Papers 643.
- Guggenberger N., 'Essential Platforms' (2020) SSRN <https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3703361> accessed 9 October 2020.
- Gutwirth S. and de Hert P., 'Regulating Profiling in a Democratic Constitutional States' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* 271 (Springer 2006)
- Habermas J., 'Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research' (2006) 16(4) Communication Theory 411.
- Habermas J., *Between Facts and Norms* (MIT Press 1998).
- Habermas J., *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* 210 (MIT Press 1991).
- Halpin E. and Simpson S., 'Between Self-Regulation and Intervention in the Networked Economy: The European Union and Internet Policy' (2002) 28(4) Journal of Information Science 285.
- Hardy I.T., 'The Proper Legal Regime for "Cyberspace"' (1994) 55 University of Pittsburgh Law Review 993.
- Hartmut R., *Social Acceleration: A New Theory of Modernity* (Columbia University Press 2013).
- Hartzog W. and Richards N., 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687.
- Hartzog W., 'Website Design as Contract' (2011) 60(6) American University Law Review 1635.
- Hartzog W., Melber A. and Salinger E., 'Fighting Facebook: A Campaign for a People's Terms of Service' Center for Internet and Society (22 May 2013) http://cyberlaw.stanford.edu/blog/2013/05/fighting-facebook-campaign-people%E2%809699s-terms-service.
- Harvey E. and Others (eds), *Private Life and Privacy in Nazi Germany* (Cambridge University Press 2019).
- Helberger N. and others, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34(1) The Information Society 1.
- Helberger N., 'Diversity by Design' (2011) 1 Journal of Information Policy 441.
- Helberger N., 'On the Democratic Role of News Recommenders' (2019) 7(8) Digital Journalism 993.
- Helmond A., 'The Platformization of the Web: Making Web Data Platform Ready' (2015) 1(2) Social Media + Society 1.
- High-Level Group on Media Freedom and Pluralism, 'A Free and Pluralistic Media to Sustain European Democracy' (2013) https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/HLG%20Final%20Report.pdf
- High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.
- Hijmans H., *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU* (Springer 2016).

- Hildebrandt M. and Gutwirth S. (eds), *Profiling the European Citizen. Cross-Disciplinary Perspectives* (Springer 2008).
- Hildebrandt M. and O'Hara K. (eds), *Life and the Law in the Era of Data-Driven Agency* (Edward Elgar 2020).
- Hildebrandt M., 'Slaves to Big Data. Or Are We?' (2013) 17 IDP Revista de Internet Derecho y Política 7.
- Hildebrandt M., *Smart Technologies and the End(s) of Law* (Edward Elgar 2016).
- Hildebrandt M., 'The Artificial Intelligence of the European Union' (2020) 21 German Law Journal 73.
- Hildebrandt M., 'The Dawn of a Critical Transparency Right for the Profiling Era', in Jacques Bus and others (eds), *Digital Enlightenment Yearbook* (IOS Press 2012).
- Hirsch D.D., 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439.
- Hirschl R. and Shachar A., 'Spatial Statism' (2019) 17(2) International Journal of Constitutional Law 387.
- Ho D.E. and Schauer F., 'Testing the Marketplace of Ideas' (2015) 90 New York University Law Review 1161.
- Hong Y., *Networking China: The Digital Transformation of the Chinese Economy* (University of Illinois Press 2017).
- Humerick M., 'Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2018) 34 Santa Clara High Technology Law Journal 393.
- Husovec M., 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (2017) 12(2) Journal of Intellectual Property Law and Practice 115.
- Husovec M., 'How Europe Wants to Redefine Global Online Copyright Enforcement' in Tatiana E. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* 513 (Wolter Kluwer 2019).
- Martin Husovec, *Injunctions Against Intermediaries in the European Union* (Cambridge University Press 2017).
- Husovec M., *Injunctions Against Intermediaries in the European Union* (Cambridge University Press 2017).
- IGF Dynamic Coalition, 'Best Practices on Platforms' Implementation of the Right to an Effective Remedy' (2018) https://www.intgovforum.org/multilingual/content/dcpr-best-practices-on-due-process-safeguards-regarding-online-platforms'-implementation-of.
- Ingram M., 'How Google and Facebook Have Taken Over the Digital Ad Industry' Fortune (4 January 2017) https://fortune.com/2017/01/04/google-facebook-ad-industry/.
- Ip E.C., 'Globalization and the Future of the Law of the Sovereign State' (2010) 8(3) International Journal of Constitutional Law 636.
- Irti N. and Severino E.*, Dialogo su diritto e tecnica* (Laterza 2001).
- Jackson V.C. and Tushnet M. (eds), *Proportionality: New Frontiers, New Challenges* (Cambridge University Press 2017).
- Jaffe L., 'Law Making by Private Groups' (1937) 51 Harvard Law Review 201.
- Jain P., Gyanchandani M. and Khare N., 'Big Data Privacy: A Technological Perspective and Review' (2016) 3 Journal of Big Data 25.
- Jančiūtė L., 'EU Data Protection and "Treaty-base Games": When Fundamental Rights are Wearing Market-making Clothes' in Ronald Leenes and Others (eds), *Data Protection and Privacy. The Age of Intelligent Machine* (Hart 2017).
- Janeček V. and Malgieri G., 'Data Extra Commercium' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance—Contract Law 2.0?* 93 (Hart 2020).

- Jenkins H., *Convergence Culture: Where Old and New Media Collide* (New York University Press 2006).
- Johnson D.R. and Post D., 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367.
- Johnston L. and Shearing C., *Governing Security. Explorations in Policing and Justice* (Routledge 2003).
- Joint industry statement of 17 March 2020 of Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter and YouTube on working together to combat misinformation (16 March 2020) https://about.fb.com/news/2020/06/coronavirus/.
- Jones M.L., 'Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216.
- Jozwiak M., 'Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union. The Vulnerability of Rights in an Online Context' (2016) 23(3) Maastricht Journal of European and Comparative Law 404.
- Kaiser B., *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper Collins 2019).
- Kaltheuner F. and Bietti E., 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2(2) Journal of Information Rights, Policy and Practice.
- Kaminski M., 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529.
- Kaminski M.E., 'The Right to Explanation, Explained' (2019) 34 Berkley Technology Law Journal 189.
- Kaplan C.S., 'A Kind of Constitutional Convention for the Internet' The New York Times (23 October 1998) http://www.nytimes/com/library/tech/98/10/cyber/cyberlaw/23law.html.
- Karapapa S. and Borghi M., 'Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm' (2015) 23 International Journal of Law & Information Technology 261.
- Karppinen K., 'The Limits of Empirical Indicators: Media Pluralism as an Essentially Contested Concept' in Peggy Valcke and others (eds), *Media Pluralism and Diversity: Concepts, Risks and Global Trends* 287 (Springer 2015).
- Kaye D., *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019).
- Keane M. and Yu H., 'A Digital Empire in the Making: China's Outbound Digital Platforms' (2019) 13 International Journal of Communication 4624.
- Keller D., 'The Right Tools: Europe's Intermediary Liability Laws and the Eu 2016 General Data Protection Regulation' (2018) 33 Berkley Technology Law Journal 297.
- Keller D., 'Who Do You Sue? State and Platform Hybrid Power Over Online Speech' (2019) Hoover Institution, Aegis Series Paper No. 1902 https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf.
- Keller T.R. and Gillett R., 'Why is it so Hard to Stop COVID-19 Misinformation Spreading on Social Media?' The Conversation (13 April 2020) https://theconversation.com/why-is-it-so-hard-to-stop-covid-19-misinformation-spreading-on-social-media-134396.
- Kerr O.S., 'The Mosaic Theory of the Fourth Amendment' (2012) 111 Michigan Law Review 311.

- Kessler F., 'Contract of Adhesion - Some Thoughts about Freedom of Contract' (1943) 43 Columbia Law Review 629.
- Kim N.S. & D. A. Telman, 'Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent' (2015) 80 Missouri Law Review 723.
- Kindt E.J., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis* (Springer 2013).
- Kirkpatrick M., 'Facebook's Zuckerberg Says the Age of Privacy is Over' The New York Times (10 January 2010) https://www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html?source=post_page.
- Kitchin R. and Lauriault T.P., 'Small Data, Data Infrastructures and Big Data' (2014) 80(4) GeoJournal 463.
- Klabbers J., Peters A. and Ulfstein G., *The Constitutionalisation of International Law* (Oxford University Press 2008).
- Klang M. and Andrew Murray (eds), *Human Rights in the Digital Age* (Cavendish 2005).
- Klonick K., 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) 129(8) The Yale Law Journal 2232.
- Klonick K., 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598.
- Knight W., 'China Plans to Use Artificial Intelligence to Gain Global Economic Dominance by 2030' MIT Technology Review (21 July 2017) https://www.technologyreview.com/2017/07/21/150379/ china-plans-to-use-artificial-intelligence-to-gain-global-economic-dominance-by-2030/.
- Knox J.H., 'Horizontal Human Rights Law' (2008) 102(1) American Journal of International Law 1.
- Kokott J. and Sobotta C., 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.
- Koltay A., *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere* (Hart 2019).
- Koops B.J., 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250.
- Kosseff J., 'Defending Section 230: The Value of Intermediary Immunity' (2010) 15 Journal of Technology Law & Policy 123.
- Kosseff J., *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).
- Kostka G., 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' (2019) 21(7) New Media & Society 1565.
- Kreimer S.F., 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 University of Pennsylvania Law Review 11.
- Kroll J.A. and others, 'Accountable Algorithms' (2016) 165 University of Pennsylvania Law Review 633.
- Kuczerawy A. and Ausloos J., 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Columbia Technology Law Journal 219.
- Kuczerawy A., 'Intermediary liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (2015) 31(1) Computer Law & Security Review 46.
- Kuczerawy A., 'Safeguards for Freedom of Expression in the Era of Online Gatekeeping' (2018) 3 Auteurs & Media 292.

- Kuczerawy A., 'The Power of Positive Thinking. Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression' (2017) 3 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 182.
- Kuczerawy A., 'The Proposed Regulation on Preventing the Dissemination of Terrorist Content Online: Safeguards and Risks for Freedom of Expression' (2018) CITIP paper for the Center for Democracy and Technology, https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf.
- Kulk S. & Zuiderveen Borgesius F., 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34(11) European Intellectual Property Review 791.
- Kumm M. and Ferreres Comella V., 'What Is So Special about Constitutional Rights in Private Litigation? A Comparative Analysis of the Function of State Action Requirements and Indirect Horizontal Effect' in Andras Sajó and Renata Uitz (eds), T*he Constitution in Private Relations: Expanding Constitutionalism* 265 (Eleven 2005).
- Kumm M. and Walen A.D., 'Human Dignity and Proportionality: Deontic Pluralism in Balancing' Grant Huscroft and others (eds), *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (Cambridge University Press 2014).
- Kumm M., 'Constituent Power, Cosmopolitan Constitutionalism, and Post-Positivist Law' (2016) 14(3) International Journal of Constitutional Law 2016.
- Kuner C. and others, 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 6 International Data Privacy Law 167.
- Kuner C. and others, 'Risk Management in Data Protection' (2015) 5(2) International Data Privacy Law 95
- Kuner C., 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235.
- Kuner C., 'The Internet and the Global Reach of EU Law', in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019).
- Laidlaw E.B., 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24(3) International Review of Computer Law and Technology 263.
- Laney D., '3D Data Management: Controlling Data Volume, Velocity and Variety' (2001) Application Delivery Strategies.
- Langvardt K., 'Regulating Online Content Moderation' (2018) 106 The Georgetown Law Journal 1353.
- Lawson G., 'The Rise and Rise of the Administrative State' (1994) 107 Harvard Law Review 1231.
- Leczykiewicz D., 'Horizontal Application of the Charter of Fundamental Rights' (2013) 38(3) European Law Review 479
- Lenaerts K., 'Exploring the Limits of the EU Charter of Fundamental Rights' (2013) 8(3) European Constitutional Law Review 375.
- Lessig L. and Resnick P., 'Zoning Speech on the Internet: A Legal and Technical Model' (1998) 98 Michigan Law Review 395.
- Lessig L., 'An Information Society: Free or Feudal' (2004) World Summit on the Information Society (WSIS), http://www.itu.int/wsis/docs/pc2/visionaries/lessig.pdf.
- Lessig L., 'The New Chicago School' (1998) 27(2) The Journal of Legal Studies 661.
- Lessig L., *Code: And Other Laws of Cyberspace* Version 2.0 (Basic Books 2006)
- Lessin J., 'Facebook Shouldn't Fact Check. New York Times', The New York Time (29 November 2016) https://www.nytimes.com/2016/11/29/opinion/facebook-shouldnt-fact-check.html.
- Liang F. and others, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure' (2018) 10(4) Policy & Internet 415.
- Lidsky L.B., 'Public Forum 2.0' (2011) Boston University Law Review 1975.

- Linskey O., 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 (1) Theoretical Inquiries in Law 189.
- Linz J.J., *Totalitarian and Authoritarian Regimes* (Lynne Rienner 2000).
- Lloyd I., 'From Ugly Duckling to Swan. The Rise of Data Protection and its Limits' (2018) 34 Computer Law & Security Review 779.
- Lobel O., 'The Law of the Platforms' (2016) 101 Minnesota Law Review 87.
- Lohr S., *Data-Ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else* (Blackstone 2015).
- Loi M. and Dehaye P.O., 'If Data is the New Oil, when is the Extraction of Value from data Unjust?' (2018) 7(2) Philosophy & Public Issues 137.
- Lombardi G., *Potere privato e diritti fondamentali* (Giappichelli 1970).
- Lucchi N., 'Freedom of Expression and the Right to Internet Access', in Monroe E. Price, Stefaan G. Verhulst and Libby Morgan (eds), *Routledge Handbook of Media Law* (Routledge 2013).
- Luciani M., 'La libertà di informazione nella giurisprudenza costituzionale italiana' (1989) (4) Politica del diritto 605.
- Lynskey O., 'Regulating Platform Power' (2017) LSE Legal Studies Working Paper 1 http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf.
- Lynskey O., 'Control Over Personal Data in A Digital Age: Google Spain v AEPD And Mario Costeja Gonzalez' (2015) 78 Modern Law Review 522.
- Lynskey O., 'Regulation by Platforms: The Impact on Fundamental Rights' in Luca Belli and Nicolo Zingales (eds), *Platform Regulations How Platforms are Regulated and How They Regulate Us* (FGV Direito Rio 2017).
- Lynskey O., *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
- Lyon D., *Surveillance After Snowden* (Polity Press 2015).
- Lyon D., *The Culture of Surveillance: Watching as a Way of Life* (Polity Press 2018).
- Maceinate M., 'The "Riskification" of European Data Protection Law through a two-fold Shift' European Journal of Risk Regulation (2017) 8(3) European Journal of Risk Regulation 506.
- MacKinnon R., *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2013).
- Macnish K., 'Unblinking Eyes: The Ethics of Automating Surveillance' (2012) 14 Ethics and Information Technology 151.
- Malgieri G. and Comandè G., 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 234.
- Malgieri G., 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35(5) Computer Law & Security Review 105327.
- Manetti M., 'La libertà di manifestazione del pensiero' in Roberto Nania and Paolo Ridola (eds), *I diritti costituzionali,* vol. II, 549 (Giappichelli 2001).
- Manetti M., 'Liberta di pensiero e anonimato in rete' (2014) (1) Diritto dell'informazione e dell'informatica 139.
- Mann M. and Matzner T., 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6(2) Big Data & Society https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805.
- Mann M., 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia' (2018) 80 International Communication Gazette 369.

- Mansell R. and Javary M., 'Emerging Internet Oligopolies: A Political Economy Analysis' in Arthur S. Miller and Warren J Samuels (eds), *An Institutionalist Approach to Public Utilities Regulation* (Michigan State University Press 2002).
- Mantelero A., 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor and Others (eds), *Group Privacy* (Springer 2017).
- Mantelero A., 'La responsabilità on-line: il controllo nella prospettiva dell'impresa' (2010) (3) Diritto dell'informazione e dell'informatica 405.
- Mantelero A., 'The Future of Consumer Data Protection in the EU Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30(6) Computer Law & Security Review 643.
- Manyika J. and others, 'Big Data: The Next Frontier for Innovation, Competition, and Productivity', McKinsey Global Institute (2011) https://www.mckinsey.com/business-functions/ mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation.
- Maple C., 'Security and Privacy in Internet of Things' (2017) 2 Journal of Cyber Policy 155.
- Marks S., *The Riddle of All Constitutions: International Law, Democracy, and the Critique of Ideology* (Oxford University Press 2004).
- Marsden C., *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011).
- Marsocci P., 'Lo spazio di Internet nel costituzionalismo' (2011) (2) costituzionalismo.it https://www.costituzionalismo.it/lo-spazio-di-internet- nel-costituzionalismo/.
- Martinelli S., *Diritto all'oblio e motori di ricerca* (Giuffrè 2017).
- Mastroianni R. and Strozzi G., 'Commento all'art. 11' in Roberto Mastroianni et al. (eds), *Carta dei diritti fondamentali dell'Unione Europea* 217 (Giuffrè 2017).
- Mastroianni R., 'I diritti fondamentali dopo Lisbona tra conferme europee e malintesi nazionali' (2010) (4) Diritto Pubblico Comparato ed Europeo XXI.
- Matthias A., 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) 6(3) Ethics and Information Technology 175.
- Mayer-Schönberger V. and Cukier K., *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).
- Mayer-Schönberger V., 'The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship' (2010) 6(2) Journal of Law and Policy for the Information Society 153.
- Mcdonald A.M. and Cranor L.F., 'The Cost of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 543.
- McIlwain C.H., *Constitutionalism: Ancient and Modern* (Amagi 2007).
- McLuhan M., *Understanding Media. The Extensions of Man* (MIT Press 1994).
- McPherson M., Smith-Lovin L. and Cook J.M., 'Birds of a Feather: Homophily in Social Networks' (2001) 27 Annual Review of Sociology 415.
- McStay A. and Urquhart L., 'This Time with Feeling? Assessing EU Data Governance Implications for Out of Home Emotional AI' (2019) 24(10) First Monday https://firstmonday.org/ojs/ index.php/fm/article/download/9457/8146.
- Meiklejohn A., 'The First Amendment is an Absolute' (1961) The Supreme Court Review 245.
- Meiklejohn A., *Free Speech and its Relation to Self-Government* (Lawbook Exchange 2011).
- Meldman J.A., 'Centralized Information Systems and the Legal Right to Privacy' (1969) 52 Marquette Law Review 335.
- Mendez R., 'Google case in Italy' (2011) 1(2) International Data Privacy Law 137.

- Mendoza I. and Bygrave L.A., 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiani Synodinou and other (eds), EU *Internet Law: Regulation and Enforcement* 77 (Springer 2017).
- Mezzanotte F., 'I poteri privati nell'odierno diritto dello sviluppo economico' (2018) (3) Politica del diritto 507.
- Mezzanotte M., 'Nuovi media e libertà antiche: la libertà di associazione in Internet' in Tommaso E. Frosini and others (eds), *Diritti e libertà in Internet* 231 (Le Monnier 2015).
- Mezzanotte M., *Il diritto all'oblio. Contributo allo studio della* privacy *storica* (Editoriali scientifiche 2009).
- Mill J.S., *On Liberty* (1859).
- Miller A.R., 'Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society' (1969) 67 Michigan Law Review 1089.
- Milton J., *Aeropagitica* (1644).
- Mittelstadt B. and Floridi L., 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303.
- Mittelstadt B., 'From Individual to Group Privacy in Big Data Analytics' (2017) 30(4) Philosophy and Technology 475.
- Mittelstadt B. and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society https://journals.sagepub.com/doi/full/10.1177/2053951716679679.
- Moazed A. and Johnson N.L., *Modern Monopolies: What It Takes to Dominate the 21st Century Economy* (St Martin's Press 2016).
- Moeller J. and Helberger N., 'Beyond the Filter Bubble: Concepts, Myths, Evidence and Issues for Future Debates. A Report Drafted for the Dutch Media Regulator' (2018) https://dare.uva.nl/search?identifier=478edb9e-8296-4a84-9631- c7360d593610.
- Moerel L., '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?' (2011) 1(1) International Data Privacy Law 28.
- Möller J. and other, 'Do not Blame it on the Algorithm: An Empirical Assessment of Multiple Recommender Systems and their Impact on Content Diversity' (2018) 21(7) Information, Communication & Society 959.
- Montagnani M.L., *Internet, contenuti illeciti e responsabilità degli intermediari* (Egea 2018)
- Moore M. and Tambini D. (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).
- Morozov E., *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2011).
- Mortelmans K., 'The Common Market, the Internal Market and the Single Market, What's in a Market?' (1998) 35(1) Common Market Law Review 101.
- Mourby M. and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review 222.
- Mueller M., 'About the Chinese "reinvention" of the Internet… Internet Governance Project blogpost' Internet Governance Project (30 March 2020) https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/.
- Mueller M., 'Hyper-Transparency and Social Control: Social Media as Magnets for Regulation' (2016) 39(9) Telecommunications Policy 804.
- Murray A., 'Internet Regulation', in David Levi-Faur (ed.), *Handbook on the Politics of Regulation* (Edward Elgar 2011).
- Murray A., 'Nodes and Gravity in Virtual Space' (2011) 5(2) Legisprudence 195.
- Murray A., *Information Technology Law: The Law and Society* (Oxford University Press 2013).

- Murray A., *The Regulation of Cyberspace* (Routledge 2007).
- Musiani F., 'Network Architecture as Internet Governance' (2013) 2(4) Internet Policy Review https://policyreview.info/node/208/pdf.
- Nahmias Y. and Perel M., 'The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations' SSRN (24 April 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3565025.
- Nannipieri L., 'Costituzione e nuove tecnologie: il caso dell'accesso ad Internet' (2013) Gruppo di Pisa https://www.gruppodipisa.it/images/rivista/pdf/Lorenzo_Nanniperi_-_Costituzione_e_nuove_ tecnologie_profili_costituzionali_dell_accesso_ad_Internet.pdf.
- Napoli P.M., *Social Media and the Public Interest: Media Regulation in the Disinformation Age* (Columbia University Press 2019).
- Narayanan A. and Shmatikov V., 'Myths and Fallacies of Personally Identifiable Information' (2010) 53 Communications of the ACM 24.
- Negroponte N., *Being Digital* (Alfred A Knopf 1995).
- Nemitz P., 'Constitutional Democracy and Technology in the age of Artificial Intelligence' (2018) 376 Philosophical Transaction of the Royal Society A.
- Netanel N.W., 'Cyberspace Self-Governance: A Skeptical View from the Liberal Democratic Theory' (2000) 88 California Law Review 401.
- Newell S. and Marabelli M., 'Strategic Opportunities (and Challenges) of Algorithmic Decision- making: A Call for Action on The Long-Term Societal Effects of 'Datification' (2015) 24 The Journal of Strategic Information Systems 3.
- Newman L.H., 'Russia Takes a Big Step Toward Internet Isolation' Wired (1 May 2020) https://www.wired.com/story/russia-internet-control-disconnect-censorship/.
- Neyland D., 'Bearing Accountable Witness to the Ethical Algorithmic System' (2016) 41 Science, Technology & Human Values 50.
- Nicas J., 'YouTube Tops 1 Billion Hours of Video a Day, on Pace to Eclipse TV' Wall Street Journal (27 February 2017) https://www.wsj.com/articles/youtube-tops-1-billion-hours-of-video-a-day-on-pace-to-eclipse-tv-1488220851.
- Niger S., 'Internet, democrazia e valori costituzionali' (2012) 153(4) Astrid http://www.astrid-online.it/rassegna/ 2012/23_02_2012.html.
- Niger S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* (Cedam 2006)
- Nissenbaum H., 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32.
- Nissenbaum H., 'From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?' (2011) 26 Berkley Technology Law Journal 1367.
- Nissenbaum H., 'Protecting Privacy in a Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.
- Nisticò M. and Passaglia P. (eds), *Internet e Costituzione* (Giappichelli 2014).
- Noble S.U., *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018).
- Novick S., *Honorable Justice* (Laurel 1990).
- Nunziato D.C., 'The Death of The Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115.
- OECD, 'China appears on course to match OECD R&D intensity by 2020' http://www.oecd.org/ sti/DataBrief_MSTI_2018.pdf.
- OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
- OECD, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives' (2011) http://www.oecd.org/internet/ieconomy/48685066.pdf.

- OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
- Ohm P., 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701
- Orofino M, 'L'inquadramento costituzionale del web 2.0: da nuovo mezzo per la libertà di espressione a presupposto per l'esercizio di una pluralità di diritti costituzionali' in AA. VV. (eds), *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee* 33 (Maggioli 2013).
- Orofino M., *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione* (Giappichelli 2014).
- Orwell G., *1984* (Penguin Books 2008).
- Oswald M., 'Algorithm-Assisted Decision-making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power' (2018) 376 Philosophical Transaction Royal Society A.
- Oversight Board Bylaws (January 2020) https://about.fb.com/wp-content/uploads/2020/01/Byla ws_v6.pdf accessed
- Oversight Board Charter (September 2019) https://about.fb.com/wp-content/uploads/2019/09/ oversight_board_charter.pdf
- Pace A. and Manetti M., 'Articolo 21', in Giuseppe Branca (ed.), Commentario della Costituzione (Zanichelli 2006).
- Pace A., 'A che serve la Carta dei diritti fondamentali dell'Unione europea? Appunti preliminari' (2011) (1) Giurisprudenza costituzionale 193.
- Padovani C. and Santaniello M., *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System* (2018) 80 International Communication Gazzette 295.
- Pagallo U., 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* 331 (Springer 2012).
- Pagallo U., *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto* (Giuffrè 2008).
- Palfrey J.G., 'Four Phases of Internet Regulation' (2010) 77(3) Social Research 981.
- Papa A., *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico* (Giappichelli 2009).
- Pariser E., *The Filter Bubble: What the Internet is Hiding from You* (Viking 2011);
- Parker G.G., Marshall W. Van Alstyne and Sangett P. Choudary, *Platform Revolution – How Networked Markets are Transforming the Economy – And How to Make them Work for You* (WW Norton & Company Inc 2017).
- Pasquale F., 'From Territorial to Functional Sovereignty: The Case of Amazon' Law and Political Economy (6 December 2017) https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon accessed 8 September 2019.
- Pasquale F., 'Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines' (2008) University of Chicago Legal Forum 263.
- Pasquale F., 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487.
- Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
- Pasquale F, 'Privacy, Autonomy, and Internet Platforms' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the Modern Age, the Search for Solutions* (The New Press 2015).

- Paul K. and Vengattil M., 'Twitter Plans to Build "Decentralized Standard" for Social Networks' *Reuters* (11 December 2019) https://www.reuters.com/article/us-twitter-content/twitter-plans-to-build-decentralized-standard-for-social-networks-idUSKBN1YF2EN.
- Peguera M., 'The Shaky Ground of the Right to Be Delisted' (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 507.
- Pelino E., 'L'anonimato su internet', in Giusella Finocchiaro (eds), *Diritto all'anonimato* 296 (Cedam 2008).
- Peppet S.R., 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 85.
- Pernice I., 'Multilevel Constitutionalism and the Crisis of Democracy in Europe' (2015) 11(3) European Constitutional Law Review 541.
- Pernice I., 'The Treaty of Lisbon: Multilevel Constitutionalism in Action' (2009) 15(3) Columbia Journal of European Law 349.
- Perritt H.H., 'Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?' (1997) 12 Berkeley Technology Law Journal 413.
- Peters J., 'The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms' (2018) 32 Berkeley Technology Law Journal 988.
- Petit N., *Big Tech and the Digital Economy. The Moligopoly Scenario* (Oxford University Press 2020).
- Petkova B., 'Privacy as Europe's First Amendment' (2019) 25(2) European Law Journal 140.
- Petruso R., *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto* (Giappichelli 2019).
- Piccone V. and Pollicino O. (eds), *La Carta dei diritti fondamentali dell'Unione europea* (Editoriale scientifica 2018).
- Pietrangelo M. (eds), *Il diritto di accesso ad Internet* (Edizioni Scientifiche Italiane 2011).
- Pinelli C., '"Postverità", verità e libertà di manifestazione del pensiero' (2017) (1) Rivista di diritto dei media 4.
- Pinelli C., *Il momento della scrittura. Contributo al dibattito sulla Costituzione europea* (Il Mulino 2002).
- Pino G., *Il diritto all'identità personale* (Il Mulino 2003).
- Pitruzella G. and Pollicino O., Disinformation and Hate Speech: An European Constitutional Perspective (Bocconi University Press 2020).
- Pizzetti F. (eds)*, Il caso del diritto all'oblio* (Giappichelli 2013).
- Pizzetti F. (eds), *Intelligenza artificiale, protezione dei dati personali e regolazione* (Giappichelli 2018).
- Pizzetti F. (eds), *Internet e la tutela della persona: il caso del motore di ricerca* (Passigli Editori 2015).
- Pizzetti F., 'Fake news e allarme sociale: responsabilità, non censura' (2017) (1) Rivista di diritto dei media 48.
- Pizzetti F., 'La privacy come diritto fondamentale al trattamento dei dati personali nel Trattato di Lisbona' in Paola Bilancia And Marialisa D'Amico (eds), *La nuova Europa dopo il Trattato di Lisbona* 83 (Giuffrè 2009).
- Pizzetti F., 'La tutela della riservatezza nella società contemporanea' (2010) (1) Percorsi costituzionali 61.
- Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo* (Giappichelli 2016).

- Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016).
- Pizzorusso A., *Il patrimonio costituzionale europeo* (Il Mulino 2002).
- Plea A. for a Balanced Approach' (2011) 48 Common Market Law Review 1455.
- Pollicino O. and Apa E., *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective* (Egea 2013).
- Pollicino O. and Bassini M., 'Bridge Is Down, Data Truck Can't Get Through...A Critical View of the Schrems Judgment in the Context of European Constitutionalism' (2017) 16 Global Community Yearbook of International Law and Jurisprudence 2016 245.
- Pollicino O. and Bassini M., 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis', in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* 508. (Edward Elgar 2014).
- Pollicino O. and Bassini M., 'La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo' (2015) (4-5) Diritto dell'informazione e dell'informatica 741.
- Pollicino O. and Bassini M., 'Reconciling Right to be Forgotten and Freedom of Information in the Digital Age. Past and Future of Personal Data Protection in the EU' (2014) 2 Diritto pubblico comparato ed europeo 641.
- Pollicino O. and Bassini M., 'The Law of the Internet between Globalisation and Localization' in Miguel Maduro, Kaarlo Tuori and Suvi Sankari (eds), *Transnational Law. Rethinking European Law and Legal Thinking* 346 (Cambridge University Press 2016).
- Pollicino O. and Bassini M., *Verso un Internet Bill of Rights* (Aracne 2015).
- Pollicino O. and Bietti E., 'Truth and Deception across the Atlantic. A Roadmap on Disinformation in the US and Europe' (2019) 11(1) Italian Journal of Public Law 43.
- Pollicino O. and De Gregorio G., 'A Constitutional Driven Change of Heart. ISP Liability and Artificial Intelligence in the Digital Single Market' 18(1) The Global Community Yearbook of International Law and Jurisprudence 238.
- Pollicino O. and others, *Internet: regole e tutela dei diritti fondamentali* (Aracne 2013).
- Pollicino O. and Romeo G. (eds), *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe* (Routledge 2016).
- Pollicino O., 'Contact tracing and COVID-19: Commission and Member States agree on specifications' EU Law Live (16 June 2020) https://eulawlive.com/contact-tracing-and-covid-19-commission-and-member-states-agree-on-specifications/.
- Pollicino O., 'Fake News, Internet and Metaphors' (2017) (1) Rivista di diritto dei media 23.
- Pollicino O., 'Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech' (2019) 25 European Law Journal 155.
- Pollicino O., 'Right to Internet Access: Quid Iuris?' in Andreas von Arnauld, Kerstin von der Decken and Mart Susi (eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric* 263 (Cambridge University Press 2019).
- Pollicino O., De Gregorio G. and Somaini L., 'The European Regulatory Conundrum to Face the Rise and Amplification of False Content Online' (2020) 19(1) Global Yearbook of International Law and Jurisdprudence 319
- Popper B., 'A Quarter of the World's Population now Uses Facebook Every Month' The Verge (3 May 2017) https://www.theverge.com/2017/5/3/15535216/facebook-q1-first-quarter-2017-earnings.
- Poullet Y., 'Data Protection Between Property and Liberties. A Civil Law Approach' in Henrik W.K. Kaspersen and Anja Oskamp (eds), *Amongst Friends in Computers and*

Law. A Collection of Essays in Remembrance of Guy Vandenberghe 160 (Kluwer Law International 1990).
- Poullet Y., 'Data Protection Legislation: What is at Stake for our Society and Democracy' (2009) 25 Computer Law & Security Review 211.
- Price M.E. and Verhulst S.G., *Self-Regulation and the Internet* (Kluwer 2004).
- Pruneyard Shopping Center v Robins, 447 U.S. 74 (1980)
- Puetz T., 'Facebook: The New Town Square' (2014) 44 Southwestern Law Review 385
- Purtova N., 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.
- Purtova N., *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011).
- Puschmann C. and Burgess J., 'Big Data, Big Questions. Metaphors of Big Data' (2014) 8 International Journal of Communication 1690.
- Quattrociocchi W. and others, 'Echo chambers on Facebook' (2016) The Harvard John M. Olin Discussion Paper Series http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein _877.pdf.
- Quelle C., 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9(3) European Journal of Risk Regulation 502.
- Quintais J.P. et al., 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' (2019) 10(3) Journal of Intellectual Property, Information Technology and E-Commerce Law 277.
- Radin M.J., *Boilerplate the Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013).
- Radu R., *Negotiating Internet Governance* (Oxford University Press 2019).
- Rahman K.S., 'Monopoly Men' Boston Review (11 October 2017) http://bostonreview.net/ science-nature/k-sabeel-rahman-monopoly-men.
- Rahman K.S., 'The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept' (2018) 39 Cardozo Law Review 1621.
- Ranchordas S. and Goanta C., 'The New City Regulators: Platform and Public Values in Smart and Sharing Cities' (2020) 36 Computer Law and Security Review 105375.
- Raso F. and others, 'Artificial Intelligence & Human Rights: Opportunities & Risks' (2018) Berkman Klein Center Research Publication No. 2018-6 https://dash.harvard.edu/bitstream/handle/1/38021439/2018-09_AIHumanRights.pdf?sequence=1&isAllowed=y.
- Redeker D., Gill L. and Gasser U., 'Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights' (2018) 80(4) International Communication Gazette 302.
- Regan P.M., *Legislating Privacy, Technology, Social Values and Public Policy* 321 (University of North Carolina Press 1995).
- Reidenberg J.R., 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997-1998) 76 Texas Law Review 553.
- Reidenberg J.R., 'Governing Networks and Rule-Making Cyberspace' (1996) 45 Emory Law Journal 911.
- Reidenberg J.R., 'States and Internet enforcement' (2004) 1 University of Ottawa Law & Technology Journal 213.
- Resta G., 'Anonimato, responsabilità, identificazione: prospettive di diritto comparato' (2014) (2) Diritto dell'informazione e dell'informatica 171.
- Resta G., 'L'anonimato in Internet', in Tommaso E. Frosini 'Internet come ordinamento giuridico' (2014) (1) Percorsi costituzionali 13.

- Resta G., *Identità personale e identità digitale* (2007) (3) Diritto dell'informazione e dell'informatica 511.
- Rheingold H., 'Habermas Blows Off Question about the Internet and the Public Sphere' SmartMobs (5 November 2007) http://www.smartmobs.com/2007/11/05/habermas-blows-off-question-about-the-internet-and-the-public-sphere/.
- Riccio G.M., 'Anonimato e responsabilità in Internet' (2000) (2) Diritto dell'informazione e dell'informatica 314.
- Riccio G.M., 'Social networks e responsabilità civile' (2010) (6) Diritto dell'informazione e dell'informatica 859.
- Riccio G.M., *La responsabilità degli internet providers* (Giappichelli 2002).
- Richards N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015).
- Richards N.M. and King J.H., 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41.
- Richards N.M., 'The Information Privacy Law Project' (2006) 94 Georgetown Law Journal 1087.
- Ro J., 'Borders and Bits' (2018) 71 Vanderbilt Law Review 179.
- Roberts S.T., 'Content Moderation' in Laurie A. Schintler and Connie L. McNeely (eds), *Encyclopedia of Big Dat*a (Springer 2017).
- Roberts S.T., 'Digital detritus: "Error" and the Logic of Opacity in Social Media Content Moderation, (2018) 23(3) First Monday https://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/8283/6649.
- Roberts S.T.*, Behind the Screen. Content Moderation in the Shadows of Social Media* (Yale University Press 2019).
- Robertson V.H.S.E., 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57(1) Common Market Law Review 161.
- Robin-Olivier S., 'The 'Digital Single Market' and Neoliberalism: Reflections on Net Neutrality', in Margot E. Salomon and Bruno De Witte (eds), *Legal Trajectories of Neoliberalism: Critical Inquiries on Law in Europe* 45 (Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2019/43 2019).
- Rocher L., Hendrickx J.M. and de Montjoye Y., 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069.
- Rodotà S., 'Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali' (1997) (4) Rivista critica diritto privato 558.
- Rodotà S., 'Una Costituzione per Internet?' (2010) (3) Politica del diritto 337.
- Rodotà S., *Elaboratori elettronici e controllo sociale* (Il Mulino 1973).
- Rodotà S., *Foucault e le nuove forme del potere* (La Biblioteca di Repubblica 2011).
- Rodotà S., *Vivere la democrazia* (Laterza 2019).
- Romei A. and Ruggieri S., 'A Multidisciplinary Survey on Discrimination Analysis' (2014) 29 The Knowledge Engineering Review.
- Rosenfeld M. and Sajo A., 'Spreading Liberal Constitutionalism: An Inquiry into the Fate of Free Speech Rights in New Democracies' in Sujit Choudhry (ed.), *The Migration of Constitutional Ideas* 152 (Cambridge University Press 2007).
- Rossello C., 'Riflessioni de jure condendo in materia di responsabilità del provider' (2010) (4-5) Diritto dell'informazione e dell'informatica 617.
- Rouvroy A. and Poullet Y., 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth and others, *Reinventing Data Protection?* 45 (Springer 2009).
- Rouvroy A., 'Technology, Virtuality and Utopia: Governmentality in an Age of Autonomic Computing' in Mireille Hildebrandt and Antoniette Rouvroy, *Law, Human*

Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology (Routledge 2011).
- Rozenshtein A.Z., 'Surveillance Intermediaries' (2018) 70 Stanford Law Review 99.
- Rubinfeld D.L. and Gal M.S., 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339.
- Rubinstein I. and Good N., 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Technology Law Journal 1333.
- Rubinstein I.S., 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74.
- Rubinstein I.S., 'Regulating Privacy by Design' (2012) 26 Berkeley Technology Law Journal 1409.
- Ruggeri A, 'Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)' (2016) (3) Consulta Online 371.
- Ruggeri A., 'La "federalizzazione" dei diritti fondamentali, all'incrocio tra etica, scienza e diritto' (2019) (2) Rivista di diritto media 14.
- Ruggles R., John de J. Pemberton Jr. and Arthur R. Miller, 'Computers, Data Banks, and Individual Privacy' (1968) 53 Minnesota Law Review 211.
- Rushkoff D., *Throwing Rocks at the Google Bus* (Portfolio 2016).
- Sadowski J., 'When Data Is Capital: Datafication, Accumulation, and Extraction' (2019) 6 Big Data & Society https://journals.sagepub.com/doi/full/10.1177/2053951718820549.
- Sajó A. and Uitz R., *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).
- Sander B., 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights based Approach to Content Moderation' (2020) 43(4) Fordham Journal of International Law 939.
- Santa Clara Principles on Transparency and Accountability in Content Moderation (2018) https://santaclaraprinciples.org/.
- Santaniello M. and others, 'The Language of Digital Constitutionalism and the Role of National Parliaments' (2018) 80 International Communication Gazette 320.
- Sartor G. & Viola de Azevedo Cunha M., 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) International Journal of Law & Information Technologies 15.
- Sartor G. and Viola De Azevedo Cunha M., 'Il caso Google-Vividown tra protezione dei dati e libertà di espressione on-line' (2010) (4-5) Diritto dell'informazione e dell'informatica 645.
- Sartor G., '"Providers" Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?' (2013) 3(1) International Data Privacy Law 3.
- Sartor G., 'Providers Liability. From the eCommerce Directive to the Future' (2017) In-depth analysis for the IMCO Committee http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/ IPOL_IDA(2017)614179_EN.pdf.
- Sartori G., 'Constitutionalism: A Preliminary Discussion' (1962) 56(4) The American Political Science Review 853.
- Sassen S., 'On the Internet and Sovereignty' (1998) 5 Indiana Journal of Global Legal Studies 545.
- Sassi S., 'La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della Costituzione. Il (recente) caso dell'associazione xenofoba' in AA. VV., *Da Internet ai Social Network* 33 (Maggioli 2013).
- Scalisi A., *Il diritto alla riservatezza* (Giuffrè 2002).

- Schaurer F., *The Exceptional First Amendment,* in Michael Ignatieff (ed.), *American Exceptionalism and Human Rights* 29 (Princeton University Press 2005).
- Schermer B.W., 'The Limits of Privacy in Automated Profiling and Data Mining' (2011) 27(1) Computer Law & Security Review 45.
- Schiller D., 'Reconstructing Public Utility Networks: A Program for Action' (2020) 14 International Journal of Communication 4989.
- Schudson M., 'Was There Ever a Public Sphere? If So, When? Reflections on the American Case' in John Calhoun (ed.), *Habermas and the Public Sphere* 143 (MIT Press 1992).
- Schutze R., '"Delegated" Legislation in the (New) European Union: A Constitutional Analysis' (2011) 74(5) Modern Law Review 661.
- Schwab K., The Fourth Industrial Revolution (Crown 2016).
- Schwartz P. and Solove D., 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814.
- Schwartz P.M. and Peifer K.N., 'Transatlantic Data Privacy' (2017) 106 Georgetown Law Journal 115.
- Scott J., 'Extraterritoriality and Territorial Extension in EU Law' (2018) 62 American Journal of Comparative Law 87.
- Selbst A.D. and Powles J., 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.
- Shadmy T., 'The New Social Contract: Facebook's Community and Our Rights' (2019) 37 Boston University International Law Journal 307.
- Shapiro A., 'The Disappearance of Cyberspace and the Rise of Code' (1998) 8 Seton Hall Constitutional Law Journal 703.
- Shapiro A.L., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World we Know* 11 (Public Affairs 1999).
- Sica S. e Stanzione P., *Commercio elettronico e categorie civilistiche* (Giuffrè 2002).
- Simon H.A., 'Designing Organizations for an Information-Rich World' in Martin Greenberger (ed.), *Computers, Communications, and the Public Interest* 37 (Johns Hopkins Press 1971).
- Simoncini A., 'L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà (2019) (1) in BioLaw Journal 63.
- Simoncini A., 'Sovranità e potere nell'era digitale', in Tommaso E. Frosini and others (eds), *Diritti e libertà in Internet* 231 (Le Monnier 2015).
- Simoncini M., *Administrative Regulation Beyond the Non-Delegation Doctrine: A Study on EU Agencies* (Hart 2018).
- Sirena P. and Zoppini A. (eds), *I poteri privati e il diritto della regolazione* (Roma TrE-Press 2018).
- Slawson D., 'Standard Forms of Contract and Democratic Control of Lawmaking Power' (1967) 84 Harvard Law Review 529.
- Solon O., 'To Censor or Sanction Extreme Content? Either Way, Facebook Can't Win' The Guardian (23 May 2017) https://www.theguardian.com/news/2017/may/24/facebook-struggles-with-mission-impossible-to-stop-online-extremism.
- Solove D., *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press 2013).
- Solove D.J., 'A Brief History of Information Privacy Law' (2006) Proskauer on Privacy.
- Sommer J.H., 'Against Cyberlaw' (2000) 15 Berkeley Technology Law Journal 1145.
- Spano R., 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665.
- Spoerri T., 'On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market'

(2019) 10(2) Journal of Intellectual Property, Information Technology and E-Commerce Law 173.
- Squires C.R., 'Rethinking the Black Public Sphere: An Alternative Vocabulary for Multiple Public Spheres' (2002) 12(4) Communication Theory 446.
- Srnicek N., 'The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model' (2017) 23(4) Juncture 254.
- Srnicek N., *Platform Capitalism* (Polity Press 2016).
- Stalla-Bourdillon S. and Knight A., 'Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data' (2017) 34 Wisconsin International Law Journal 284.
- Stark B. and others, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse' Algorithm Watch (26 May 2020) https://algorithmwatch.org/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch. pdf accessed 7 June 2020.
- Stasi M.L., 'Ensuring Pluralism in Social Media Markets: Some Suggestions' (2020) EUI Working Paper RSCAS 2020/05 https://cadmus.eui.eu/bitstream/handle/1814/65902/ RSCAS_2020_ 05.pdf?sequence=1&isAllowed=y.
- Stein L., 'Policy and Participation on Social Media: The Cases of YouTube, Facebook, and Wikipedia' (2013) 6(3) Communication, Culture & Critique 353
- Stewart L., 'Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security' (2019) 60 Boston College Law Review 347.
- Stone Sweet A. and Mathews J., *Proportionality Balancing and Constitutional Governance. A Comparative and Global Approach* (Oxford University Press 2019).
- Stroud N.J., 'Polarization and Partisan Selective Exposure' (2010) 60(3) Journal of Communication 556.
- Sunstein C.R., *Democracy and the Problem of Free Speech* (The Free Press 1995).
- Sunstein C.R., *Infotopia: How Many Minds Produce Knowledge* (Oxford University Press 2006).
- Sunstein C.R., *Republic.com* (Princeton University Press 2002).
- Sunstein C.R., *Republic.com 2.0* (Princeton University Press 2007).
- Sunstein C.R.., 'Constitutionalism after the New Deal' (1987) 101 Harvard Law Review 421.
- Suzor N., 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) Social Media + Society https://journals.sagepub.com/doi/pdf/10.1177/ 2056305118787812.
- Suzor N., *Lawless: The Secret Rules That Govern our Digital Lives* (Cambridge University Press 2019).
- Svantesson D.B.J., 'Bad News for the Internet as Europe's Top Court Opens the Door for Global Content Blocking Orders' Linkedin (3 October 2019) https://www.linkedin.com/pulse/bad-news-internet-europes-top-court-opens-door-global-svantesson/
- Svantesson D.J.B., 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3(4) International Data Privacy Law 278.
- Taddeo M. and Floridi L. (eds), *The Responsibilities of Online Service Providers* (Springer 2017).
- Taddeo M., 'Modelling Trust in Artificial Agents, A First Step Toward the Analysis of E-Trust' (2010) 20 Minds and Machines 243.
- Tanzarella P., 'Accesso a Internet: verso un nuovo diritto sociale?' in Elisa Cavasino, Giovanni Scala and Giuseppe Verde, *I diritti sociali dal riconoscimento alla garanzia: il ruolo della giurisprudenza* (Editoriale scientifca 2012).

- Taylor R.B., 'Consumer-Driven Changes to Online Form Contracts' (2011-2012) 67 NYU Annual Survey of American Law 371
- Tene O. and Polonetsky J., 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal of Technology and Intellectual Property 239.
- Teubner G. 'The Project of Constitutional Sociology: Irritating Nation State Constitutionalism' (2013) 4 Transnational Legal Theory 44.
- Teubner G., 'Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?' in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism* 3 (Hart 2004)
- Teubner G., 'The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors' (2006) 69(3) Modern Law Review 327.
- Teubner G., *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press 2012).
- Teubner G., *Law as an Autopoietic System* (Blackwell 1993).
- Tewksbury D. and Rittenberg J., 'Online News Creation and Consumption: Implications for Modern Democracies' in Andrew Chadwick & Philipp N. Howard (eds), *The Handbook of Internet Politics* 186 (Routledge 2008).
- 'The World's Most Valuable Resource is no Longer Oil, but Data' The Economist (6 May 2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
- Thurman N. and Schifferes S., 'The Future of Personalization at News Websites: Lessons from a Longitudinal Study' (2012) 13(5-6) Journalism Studies 775.
- Tosi E. and Franceschelli V., *Le regole giuridiche del commercio elettronico* (Giuffrè 2003).
- Trucco L., *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano* (Giappichelli 2004)
- Trucco L., 'Identificazione e anonimato in rete' www.metakoine.it.
- Tsai C.W. and others, 'Big Data Analytics: A Survey' (2015) 2 Journal of Big Data 21.
- Tufekci Z., 'Algorithmic Harms Beyond Facebook And Google: Emergent Challenges of Computational Agency' (2015) 13 Colorado Technology Law Journal 303.
- Tully S., 'A Human Right to Access the Internet? Problems and Prospects' (2014) 14(2) Human Rights Law Review 175.
- Turilli M. and Floridi L., 'The Ethics of Information Transparency' (2009) 11(2) Ethics and Information Technology 105.
- Turkle S., 'How Computers Change the Way We Think' (2004) 50 The Chronicle of Higher Education B26.
- Turkle S., *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster Trade 1995).
- Tushnet M., 'Shelley v. Kraemer and Theories of Equality' (1988) 33 New York Law School Law Review 383
- Tushnet M., 'The Inevitable Globalization of Constitutional Law' (2009) 49 Virginia Journal of International Law 985.
- Tushnet M., 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1(1) International Journal of Constitutional Law 79.
- Tushnet R., 'Power Without Responsibility: Intermediaries and the First Amendment' (2008) 76 George Washington Law Review 986
- Tutt A., 'The New Speech' (2014) 41 Hastings Constitutional Law Quarterly 235.
- Urban J.M. and others, *Notice and Takedown in Everyday Practice* (American Assembly 2016).
- Vaihyanathan S., *Anti-Social Media* (Oxford University Press 2018).

- Van Alsenoy B., 'Allocating Responsibility Among Controllers, Processors, And "Everything In Between": The Definition of Actors and Roles in Directive 95/46' (2012) 28 Computer Law & Security Review 30.
- Van Alsenoy B., 'Liability under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 9(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 271.
- Van Loo R., 'The Corporation as Courthouse' (2016) 33 Yale Journal on Regulation 547.
- Van Loo R., 'The New Gatekeepers: Private Firms as Public Enforcers' (2020) 106 Virginia Law Review 467.
- Van der Sloot B., 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System' (2015) 31 Computer Law and Security Review 26.
- Van der Sloot B., 'Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe' (2015) 3 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 211.
- Van Dijck J. and others, *The Platform Society: Public Values in a Connective World* (Oxford University Press 2018).
- Van Dijk J. and Poell T., 'Understanding Social Media Logic' (2013) 1(1) Media and Communication 2;
- Van Eecke P., 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48(5) Common Market Law Review 1455.
- van Hoboken J., '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.
- Veale M., Binns R. and Ausloos J., 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105
- Vigevani G.E., 'Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano' (2014) (2) Diritto dell'informazione e dell'informatica 207.
- Vigevani G.E., 'Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano' (2014) (4) Danno e responsabilità 741.
- Viola de Azevedo Cunha M. and others, 'Peer-to-peer Privacy Violations and ISP liability: Data Protection in the User-generated Web' (2012) 2(2) International Data Privacy Law 50
- Volokh E., 'In Defense of the Market Place of Ideas / Search for Truth as a Theory of Free Speech Protection' (2011) 97(3) Virginia Law Review 591
- Wachter S. and Mittelstadt B., 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 494.
- Wachter S. and others, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.
- Wagner B. and others (eds), *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations* (Edward Elgar 2019).
- Wagner B., 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11(1) Policy & Internet 104.
- Wagner B., 'Understanding Internet Shutdowns: A Case Study from Pakistan' (2018) 12 International Journal of Communication 3917.
- Wagner B., *Global Free Expression: Governing the Boundaries of Internet Content* (Springer 2016).

- Wakabayashi D. and others, 'Big Tech Could Emerge from Coronavirus Crisis Stronger Than Ever' The New York Times (23 March 2020) https://www.nytimes.com/2020/03/23/technology/ coronavirus-facebook-amazon-youtube.html.
- Waldron J., 'Constitutionalism: A Skeptical View' (2012) NYU, Public Law Research Paper No. 10-87 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1722771&rec=1&srcabs=1760963 &alg=1& pos=1.
- Walker N., *Intimations of Global Law* (Cambridge University Press 2015).
- Walkila S., *Horizontal Effect of Fundamental Rights in EU Law* (European Law Publishing 2016).
- Ward J.S. and Barker A., 'Undefined By Data: A Survey of Big Data Definitions' ArXiv http://arxiv.org/abs/1309.5821.
- Warf B., 'Geographies of Global Internet Censorship' (2011) 76 GeoJournal 1.
- Warner M., *Publics and Counterpublics* (MIT University Press 2002).
- Warren S.D. and Brandeis L.D., 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
- Wauters E., Lievens E. and Valcke P., 'Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites' (2014) 22 International Journal of Law & Information Technology 254.
- Weber R.H., 'Corporate Social Responsibility as a Gap-Filling Instrument', in Andrew P. Newell (ed.). *Corporate Social Responsibility: Challenges, Benefits and Impact on Business* 87 (Nova 2014).
- Weber R.H., 'Internet of Things – New Security and Privacy Challenges' (2010) 26(1) Computer Law & Security Review 23.
- Webster J.G., 'User Information Regimes: How Social Media Shape Patterns of Consumption' (2010) 104 Northwestern University Law Review 593.
- Weiler J.H.H. and Wind M. (eds), *European Constitutionalism Beyond the State* (Cambridge University Press 2003).
- Weimar M. and Marin L., 'The Role of Law in Managing the Tension between Risk and Innovation' (2016) 7(3) European Journal of Risk Regulation 469.
- Weinberg J., 'ICANN and the Problem of Legitimacy' (2000) 50 Duke Law Journal 187.
- Weissman C.G., 'Maybe It's Time to Treat Facebook Like a Public Utility' Fast Company (1 May 2017) https://www.fastcompany.com/40414024/maybe-its-time-to-treat-facebook-like-a-public-utility.
- Werro F., 'The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash' in Aurelia Colombi Ciacchi and others (eds), *Liability in the Third Millennium, Liber Amicorum Gert Bruggemeier* 285 (Nomos 2009).
- West S.M., 'Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms' (2018) 20(11) New Media & Society 4380.
- Westin A.F., *Privacy and Freedom* (Atheneum 1967).
- Whitman J.Q., 'On Nazy "Honour" and the New European Dignity' in Christian Joerges and Navraj Singh Ghaleigh, *Darker Legacies of Law in Europe: The Shadow of National Socialism and Fascism Over Europe and Its Legal Traditions* (Hart 2003).
- Whitman J.Q., 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) Yale Law Journal 1151.
- Wiener N., *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press 1988).
- Wolfsfeld G. and others, 'Social Media and the Arab Spring: Politics Comes First' (2013) 18(2) The International Journal of Press/Politics 115.

- Wu F.T., 'Collateral Censorship and the Limits of Intermediary Immunity' (2011) 87(1) Notre Dame Law Review 293
- Wu T., 'Cyberspace Sovereignty? The Internet and the International Systems' (1997) 10(3) Harvard Law Journal 647
- Wu T., *The Attention Merchants: The Epic Scramble to Get Inside our Heads* (Knopf 2016)
- Wu T., *The Curse of Bigness: How Corporate Giants Came to Rule the World* (Atlantic Books 2020)
- Yakovleva S. and Irion K., 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation' (2020) 114 AJIL Unbound 10.
- York J.C., 'Policing Content in the Quasi-Public Sphere' Open Net Initiative' Bulletin (September 2010) https://opennet.net/policing-content-quasi-public-sphere.
- Zalnieriute M., 'Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)' (2020) 114(2) American Journal of International Law 261.
- Zanzotto F.M., 'Viewpoint: Human-in-the-loop Artificial Intelligence' (2019) 64 Journal of Artificial Intelligence Research 243.
- Zarsky T., 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 1014.
- Zarsky T., 'Social Justice, Social Norms and the Governance of Social Media' (2015) 35 Pace Law Review 154.
- Zarsky T., 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41 Science, Technology, & Human Values 118.
- Zarsky T., 'Transparent Predictions' (2013) 4 University of Illinois Law Review 1507.
- Zarsky T., 'Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375.
- Zeno-Zencovich V., 'Anonymous speech on the Internet' in Andras Koltay (ed.), *Media Freedom and Regulation in the New Media World* 103 (Wolters Kluwer 2014).
- Zeno-Zencovich V., *Freedom of Expression: A Critical and Comparative Analysis* (Routledge 2008).
- Zeno-Zencovich V., *La libertà di espressione. Media, mercato, potere nella società dell'informazione* (Il Mulino 2004).
- Ziccardi-Capaldo G., *The Pillars of Global Law* (Ashgate 2008).
- Zimmer D., 'Digital Markets: New Rules for Competition Law' (2015) 6(9) Journal of European Competition Law & Practice 627.
- Zittrain J. and Edelman B., 'Empirical Analysis of Internet Filtering in China' (2003) Harvard Law School Public Law Research Paper No. 62 https://cyber.harvard.edu/sites/cyber.harvard.edu/files/ 2003-02.pdf.
- Zittrain J., 'History of Online Gatekeeping' (2006) 19(2) Harvard Journal of Law & Technology 253.
- Zittrain J., *The Future of the Internet and How to Stop It* (Yale University Press 2008).
- Zuboff S., 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75.
- Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Polity Press 2019).
- Zuckerberg M., 'A Blueprint for Content Governance and Enforcement' Facebook (15 November 2018) https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/?hc_location=ufi.
- Zuckerberg M., 'Bringing the World Closer Together' Facebook (22 June 2017) https://www.facebook.com/notes/mark-zuckerberg/bringing-the-world-closer-together/ 10154944663901634/

- Zuckerberg M., 'Building Global Community' Facebook (16 February 2017) https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/.
- Zuiderveen Borgesius F.J. and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82.
- Zuiderveen Borgesius F.J. and others, 'Should we Worry about Filter Bubbles?' (2016) 5(1) Internet Policy Review https://policyreview.info/node/401/pdf.
- Zumbansen P., 'The Law of Society: Governance Through Contract' (2007) 14(1) Indiana Journal of Global Legal Studies 191.