2 The Rise of European Digital Constitutionalism

2.1 Moving towards European Digital Constitutionalism

The shift of the Union from a liberal perspective to a constitutional democratic approach is a story about constitutional law meeting digital technologies. The rise of European digital constitutionalism can be described as a long process if it is compared with the rampant evolution of the digital environment in the last twenty years. The turn has not been immediate but has gradually followed a path towards the integration of economic with constitutional values,[1] which define European constitutionalism,[2] while digital technologies provided opportunities to offer cross-border services and exercise individual freedoms.[3] In this transformation, a constitutional strategy complemented the internal market imprinting of the Union which is increasingly oriented to the protection of fundamental rights and democratic values.

The reason for this European constitutional shift comes from the US and European liberal approach to the digital environment at the end of the last century. Both sides of the Atlantic considered online intermediaries as neutral service providers rather than active providers. These providers do not usually produce or create content even if they host and organise information and data for profit. In other words, online intermediaries just provide digital spaces where users share their views or access services. Likewise, the advent of European data protection was

[1] Gráinne de Búrca and Joseph H. H. Weiler (eds.), *The Worlds of European Constitutionalism* (Cambridge University Press 2012).
[2] Kaarlo Tuori, *European Constitutionalism* (Cambridge University Press 2015).
[3] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006).

https://doi.org/10.1017/9781009071215.003 Published online by Cambridge University Press

considered a necessary step to ensure the free circulation of data in the internal market rather than to provide a comprehensive set of safeguards to protect privacy and personal data in the digital age.

This constitutional angle has encouraged the private sector to exploit the opportunities deriving from the use of a low-cost global communication technology for developing business models relying on a liberal approach migrating across the Atlantic. The consolidation of platform power can be considered the result of this liberal standpoint, which, at the end of the last century, encouraged private actors to gain areas of powers by processing data and information in a liberal constitutional environment. Even if the platformisation of the digital environment cannot be considered a single process,[4] it is possible to underline how the mix of this liberal approach and the development of digital technologies, primarily algorithmic systems, has enriched the functions of online platforms. The profiling of users or the organisation of content has led these actors to exercise a more pervasive control over information and data. Algorithmic technologies play a critical role in creating targeted services attracting more customers while providing precise windows of visibility and engagement for businesses and organisations to advertise their products and services.[5] To achieve this business purpose, the collection and organisation of a vast amount of data and content become a constitutive activity. The processing of information and data has entrusted these actors with almost exclusive control over online content and data, transforming their role into something more than a mere intermediary.

The consolidation of online platforms has led to a paradigmatic shift of power in the algorithmic society.[6] The private development of digital and automated technologies has not only, on the one hand, challenged the protection of individual 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

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

[5] 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).

[6] 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.

quasi-public functions in the transnational context. The setting and enforcement of private standards through algorithmic technologies or the processing of vast amounts of information raise questions about the role of (constitutional) law.[7] Digital capitalism not only affects the individual dimension but also the collective sphere as demonstrated by the Cambridge Analytica scandal.[8]

The challenges raised by digital capitalism to democratic values are one of the primary reasons leading the Union to emancipate itself from the US technological optimism which looks at the First Amendment as the dogma of digital liberalism. On the other side of the Atlantic, the characteristics of European constitutionalism have increasingly encouraged the Union to follow a new path to address the challenges of the algorithmic society. As already underlined in Chapter 1, this process can be considered the result of different constitutional premises across the Atlantic where the consolidation of digital private powers has not led to the same constitutional reaction and shift towards a democratic strategy.

Within this framework, this chapter analyses the path leading the Union to shift from a liberal approach to a democratic constitutional strategy to address the consolidation of platform powers. This chapter aims to explain the reasons for this paradigmatic shift looking at content and data as the two emblematic areas symbolising the rise of a new phase of European digital constitutionalism. This chapter focuses on three phases: digital liberalism, judicial activism and digital constitutionalism. The first part of this chapter frames 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 after the adoption of the Lisbon Treaty. The third part examines the path of the Union towards a constitutional democratic strategy and the consolidation of European digital constitutionalism.

[7] Caryn Devins and others, 'The Law and Big Data' (2017) 27 Cornell Journal of Law and Public Policy 357.

[8] 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).

2.2 The Charm of Digital Liberalism

The road of the Union towards digital liberalism has its roots in the European economic imprinting. 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 provide new possibilities for economic growth while introducing a new layer of complexity for the regulation of the internal market.

Until the adoption of the Nice Charter in 2000 and the recognition of its binding effects in 2009,[10] the European approach was firmly 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 protect society and create an equitable Internet environment'.[12] Therefore, the consolidation and harmonisation of the internal market was one of the primary drivers of the European approach at the end of the last century.

This liberal framework was also transposed in the regulation of critical areas for the growth of the digital environment. In the field of data and content, the Data Protection Directive and the e-Commerce Directive are two paradigmatic examples showing 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

[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.

processing of personal data was harmonised to promote the free circulation of personal data in the internal market. Therefore, digital technologies were considered an enabler of economic prosperity. In other words, also considering 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 digital technologies, namely digital liberalism.

Such a liberal approach does not only reflect the economic imprinting of the Union but it can also be framed within the debate about Internet regulation at the end of the last century. An extensive technological optimism from the western side of the Atlantic welcomed the advent of the Internet. As explained in Chapter 3, at that time, the digital environment was considered an area where public actors could not extend their sovereign powers and interfere with rights and freedoms. Barlow underlined that the digital space is a new world separate from the atomic dimension, where 'legal concepts of property, expression, identity, movement, and context do not apply'.[14] As for all new undiscovered worlds, the cyberspace was considered as an opportunity: a dreamland where social behaviours were not exposed to tyrannical constraints. In other words, the digital environment was considered as a new world completely separate from the atomic reality, thus preventing governments and lawmakers from exercising their traditional powers.

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] Put differently, these liberal ideas are based on a bottom-up approach: rather than relying on traditional public lawmaking powers to set the norms regulating the digital environment, digital communities would be capable of participating and creating the rules governing their online spaces.

This technological trust can also be explained by looking at the characteristics of the digital environment challenging the powers of governments and lawmakers. It is not by chance that Froomkin defines

[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).

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. As the mythical beast, the Internet has discouraged regulation since top-down attempts at regulating it (i.e. cutting off one of the Hydra's heads) would fail since communities would easily react against such interferences (i.e. 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 expression also represents some of the reasons why democratic constitutional states have adopted a free-market approach when dealing with the digital environment, while other systems have followed different paths.[18] At the end of the last century, the adoption of a paternalistic approach could have hindered the development of new digital services and the positive effects on the exercise of fundamental rights and freedoms. A strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were poised to revolutionise the entire society.

Besides, the rise of digital capitalism, or surveillance capitalism, was highly convenient not only for ensuring paths of economic growth and fostering fundamental freedoms but also for the exercise of public powers,[19] and so much so that even public actors exploited these opportunities for performing public tasks. The resilience of the liberal approach is also the result of an invisible handshake based on which governments have refrained to regulate private companies operating in the online environment to benefit from unaccountable cooperation.[20] The lack of transparency and accountability made it easier for public actors to rely on data for security and surveillance purposes, thus formally escaping constitutional safeguards. The cooperation between the public and private sector is still a relevant

[17] A. Michael Froomkin, 'The Internet as a Source of Regulatory Arbitrage' in Brian Kahin and Charles Nesson (eds.), *Borders in Cyberspace* (MIT Press 1997).

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

[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.

matter as also underlined by the Israeli Supreme Court stressing the lack of due process and the impact on freedom of expression of removal orders to social media by public authorities.[21]

The consolidation of digital liberalism across the Atlantic was primarily the result of a positive angle looking at digital technologies as an opportunity to grow and prosper when they did not represent a potential threat to individual constitutional rights and freedoms. The approach of the Union was more concerned about the potential impacts of regulatory burdens on economic (fundamental) freedoms and innovation rather than on the protection of constitutional values 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.

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 European legal framework, even if the Union has always shown its cooperative approach to the regulation of the Internet.[22] This transatlantic influence is not casual, but it is the result of the interaction between two constitutional models. Nonetheless, as underlined in Chapter 1, this relationship does not always entail the same proximity of constitutional premises. The following sections analyse the phase of digital liberalism examining the path of the Union at the beginning of this century in the field of content and data.

2.2.1 Immunising Online Intermediaries

The starting point to examine the European liberal approach in the field of content could not depart from looking at the e-Commerce Directive. 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

[21] See, e.g., *Adalah et al* v. *Israeli Ministry of Justice's Cyber Unit et al* (2021).

[22] 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.

ensuring the free movement of information society services between the Member States'.[23] 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'.[24]

This European system did not introduce a new model but was inspired by the US approach to online intermediaries, precisely the Communication Decency Act[25] and the Digital Millennium Copyright Act.[26] By recognising that online intermediaries are not involved in the creation of content, although in different ways, both these measures exempt online intermediaries from liability for transmitting or hosting unlawful third-party content.[27] When the US Congress passed Section 230 of the Communication Decency Act, one of primary aims was to encourage free expression and the development of the digital environment. In order to achieve this objective, the choice was to exempt computer service providers from liability for third-party conduct. 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 of transmitting and hosting vast amounts of content.

Since, in the lack of any legal shield, this situation would have negatively affected the development of new digital services, as some cases had already shown at that time,[28] the US policy aimed to encourage online intermediaries to grow and develop their business under the protection of the safe harbour and the Good Samaritan rule.[29] It is not by chance that Section 230 has been described as 'the twenty-six words that created the Internet'.[30] This provision has opened the door to the evolution of the digital

[23] e-Commerce Directive (n. 13), Recitals 1–3.
[24] 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.
[25] Communication Decency Act, 47 U.S.C., Section 230.
[26] Digital Millennium Copyright Act, 17 U.S.C., Section 512.
[27] Mariarosaria Taddeo and Luciano Floridi (eds.), *The Responsibilities of Online Service Providers* (Springer 2017); Graeme B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2017).
[28] *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).
[29] *Zeran* v. *Am. Online, Inc.* 129 F.3d 327, 330 (4th Cir. 1997).
[30] Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).

environment and still constitutes the basic pillar legitimising platform powers,[31] showing the primacy of the First Amendment in US constitutionalism.[32]

The US model has influenced the political choice on the eastern side of the Atlantic. The e-Commerce Directive exempts Internet service providers (or online intermediaries) from liability for the unlawful conduct of third parties.[33] Among online intermediaries,[34] 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).[35]

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 in the Convention.[37] Here, the right to freedom of expression was strictly connected to the development of new digital services. In other words, according to the Union's approach, these new technologies would constitute a 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

[31] 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.

[32] Alexander Meiklejohn, 'The First Amendment is an Absolute' (1961) 1961 The Supreme Court Review 245.

[33] Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law Review 1455; 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).

[34] This legal regime applies to three categories of online intermediaries: access providers, caching providers and hosting providers. e-Commerce Directive (n. 13), Arts. 12–14.

[35] 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* 84 (Edward Elgar 2020).

[36] e-Commerce Directive (n. 13), Recital 9.

[37] European Convention on Human Rights (1950), Art. 10.

[38] e-Commerce Directive (n. 13), Recital 42.

e-Commerce Directive does not only exempt online intermediaries from liability but also sets forth a general rule banning general monitoring imposed by Member States.[39]

Therefore, online intermediaries cannot be required to monitor the information transmitted or stored by users within their services, as well as seek facts or circumstances that reveal illegal activities conducted by their users through the relevant service.[40] This rule aims to avoid disproportionate interferences with the economic freedoms of online intermediaries which would be required to set additional financial and human resources, de facto making their activities not profitable due to the vast amount of content they transmit or host. Likewise, the ban on general monitoring also protects users' rights and freedoms by precluding public authorities from imposing surveillance obligations onto online intermediaries. Nonetheless, these limits only apply to public actors while online intermediaries enjoy margins of freedom in implementing voluntary measures to manage their digital spaces.

This legal regime highlights the architecture of freedom on which online intermediaries have been able to develop their business, and powers. These actors 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 looks reasonable as long as online intermediaries only performed passive activities, such as providing access or space to host third-party content. However, e-commerce marketplaces, search engines and social networks organising and moderating content through artificial intelligence technologies have 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 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 areas of private powers in the internal market.

Furthermore, as examined in Chapter 3, by imposing upon hosting providers the obligation to remove online content based on their

[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).

awareness or control, this system of liability has entrusted online platforms with the power to autonomously decide whether to remove or block online content. 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 escape liability 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.

This system leaves platforms free to organise content based on the logic of moderation which is driven by profit maximisation. It works as a legal shield for online platforms[42] and, even more importantly, has encouraged private actors to set their rules to organise and moderate content based on business interests and other discretionary (but opaque) conditions.[43] The organisation of content driven by unaccountable business purposes can be considered one of the primary reasons explaining how online platforms shape the protection of fundamental rights and freedoms in the digital environment. As the next subsection shows, even the European approach to personal data has played a critical role in the rise of private powers in the digital age.

2.2.2 Ensuring the Free Circulation of Personal Data

At first glance, the Union has not adopted a liberal approach to personal data. Unlike 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]

[41] 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 K. 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.

As Chapter 6 will explain in more detail, the rise of European data protection law can be examined looking at the consolidation of the constitutional dimension of privacy and the protection of personal data in the framework of the Council of Europe and Member States' national legislation.[45] 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.[46] Even before the advent of artificial intelligence technologies, the aim of this instrument, subsequently modernised in 2018,[47] was to ensure the protection of personal data taking account of the increasing flow of information across frontiers.

The Data Protection Directive could perfectly fit within this framework of safeguards and guarantees. In 1995, the adoption of the Data Protection Directive could be considered the result of a constitutional reaction against the challenges raised by the information society, as also underlined by the approach of the Council of Europe. However, a closer look can reveal how the Union policy was 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.[48] The liberal imprinting and functional approach of data protection can be understood by focusing on the first proposal of the Commission in 1990.[49] 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'.[50] Although the processing of personal data shall serve mankind and aim to protect the

[45] See, e.g., the *Datenschutzgesetz* adopted on 7 October 1970 in Germany; *Datalagen* adopted on 11 May 1973 in Sweden; Loi n. 78–17 on 6 January 1978 in France; Data Protection Act 1984 on 12 July 1984 in UK.

[46] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

[47] Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (2018).

[48] Data Protection Directive (n. 13), Recital 3.

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

[50] Ibid., 4.

privacy of data subjects,[51] the economic-centric frame of the European approach with regard to the protection of personal data cannot be disregarded.

Likewise, the Data Protection Directive does not seem to adopt a liberal approach also when looking at the principle of consent which, apparently, limits the possibility for data controllers to freely process personal data while requiring data controllers to comply with specific legal bases. The principle of consent in European data protection law ensures that data subjects can freely decide whether and how their personal data can be processed.[52] However, this liberal premise fostering autonomy and self-determination also implies that data subjects are autonomous and informed. And this would be possible thanks to the role of data protection in mitigating information asymmetry through transparency obligations and procedural safeguards. Nonetheless, despite the logic of this system, the principle of consent has not played a critical role to limit the discretion of data controllers which can rely on an alternative legal basis to process personal data or exploit their economic position, thus making consent a mandatory step and not a free choice for data subjects. This situation shows the relevance of consent, while underlining its limit and crisis in the digital age.[53]

Therefore, the European liberal approach in the field of data is counterintuitive. Despite the adoption of safeguards to deal with the processing of personal data, the European strategy aimed to reach internal market purposes, thus becoming the primary trigger of European data protection law. However, this approach should not surprise because this path was mandatory at that time. In 1995, the lack of a European constitutional framework protecting privacy and data protection was a limit to the constitutional scope of the Data

[51] Ibid., Recital 2.

[52] 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 (eds.) *Reinventing Data Protection?* 45 (Springer 2009).

[53] Gabriela Zanfir-Fortuna, 'Forgetting About Consent: Why The Focus Should Be on "Suitable Safeguards" in Data Protection Law' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.) *Reloading Data Protection* 237 (Springer 2014); Bert-J. Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250; Bart. W. Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16 Ethics and Information Technology 171.

Protection Directive which was based on the internal market clause.[54]

Besides, like in the field of content, the Union 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 primarily 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. Although it was reasonable not to foresee serious concerns at that time due to the passive nature of online intermediaries, this consideration does not explain why the first proposal to revise European data protection law has been proposed only in 2012,[55] and the GDPR entered into force in 2016, even having binding effects until 2018.[56]

In the years after the adoption of the Data Protection Directive, the Union did not make 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 amendment in more than twenty years could explain why European data protection law has failed to face the challenges raised by new ways of processing personal data in the digital environment. 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 enter 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

[54] 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).

[55] 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.

[56] 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.

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 a 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 margins of Member States were limited in relation to the liability of online intermediaries. Besides, the Union introduced other legal instruments to tackle illicit content.[57] Whereas, in the framework of data, several Member States had 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 State as demonstrated by the case of France and Germany.[58] Therefore, the heterogeneous legal system of data protection in Europe coming from the mix of different domestic traditions and margins of discretion left by the Data Protection Directive to 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 left enough space for private actors to turn their freedoms into 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 private powers in the algorithmic society have been encouraged by liberal goals and design as well as regulatory omissions. This expression of digital liberalism has played a critical role in the consolidation of digital private powers while also encouraging the rise of a new European constitutional strategy.

[57] 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.

[58] 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.

2.3 Judicial Activism As a Bridge

The rampant evolution of the digital environment at the beginning of this century has started to challenge the liberal imprinting of the Union. At the very least, two macro-events have questioned the phase of digital liberalism and opened the door to a new step in the European constitutional path characterised by the creative role of the ECJ in framing fundamental rights in the digital environment.[59] The first event triggering this phase of judicial activism concerns the rise and consolidation of new private actors in the digital environment. The second is related to recognition of the Charter as a bill of rights of the Union after the adoption of the Lisbon Treaty.[60]

Firstly, since the end of the last century, 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 to offer products and information and data, primarily through online platforms.[61] In other words, from a mere channel of communication and hosting, the Internet became a social layer where freedoms and powers interact. Within this framework, new business models have started to emerge by benefiting from the characteristics of this global channel of communication.

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 profit from the processing and analysis of information and data which attract different forms of revenue such as advertising or allow them to increasingly attract new customers to their products and services.[62] In the case of social media, these actors need to firmly govern their digital spaces by implementing automated decision-making technologies to moderate online content

[59] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart 2021).

[60] Sionhaid Douglas-Scott, 'The European Union and Human Rights after the Treaty of Lisbon' (2011) 11(4) Human Rights Law Review 645: Grainne De Burca, 'The Road Not Taken: The EU as a Global Human Rights Actor' (2011) 105(4) American Journal of International Law 649.

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

[62] Martin Moore and Damian Tambini (eds.), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).

and process data.[63] These systems help online platforms attracting revenues from the profiling of users by ensuring a healthy and efficient online community, thus contributing to corporate image and showing a commitment to ethical values. The increasing involvement of online platforms in the organisation of content and the profiling of users' preferences through the use of artificial intelligence technologies has transformed their role as hosting providers.

Secondly, the other primary driver of judicial activism, and of European digital constitutionalism, consisted of the adoption of the Lisbon Treaty which recognised the Charter as EU primary law. This step has contributed to codifying the constitutional dimension of the European (digital) environment.[64] 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.[65] The Strasbourg Court has played a crucial role not only in protecting the aforementioned fundamental rights but also in underlining the constitutional challenges coming from digital technologies.[66] 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 has limited the dialogue between the two systems,[67] thus leaving Member States to deal with the Convention within their own domestic systems. However, the relationship between the Union and the Council of Europe is closer when looking at the judicial interaction between the ECJ and the ECtHR.[68]

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

[64] Consolidated version of Treaty on the European Union (2012) OJ C 326/13, Art 6(1).

[65] Convention (n. 37), Arts. 8, 10.

[66] 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.

[67] 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).

[68] 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.

The Lisbon Treaty has constituted a crucial step allowing the right to freedom of expression,[69] private and family life,[70] and the protection of personal data,[71] as already enshrined in the Charter, to become binding vis-à-vis Member States and European institutions,[72] which can interfere with these rights only according to the conditions established by the Charter.[73] Besides, similarly to the Convention,[74] the Charter adds another important piece of the European constitutional puzzle by prohibiting the abuse of rights, which consists 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'.[75] In this sense, the evolution of European constitutional law is peculiar since the constitutional protection of fundamental rights and freedoms comes from the evolution of the European economic identity.

Within this new constitutional framework, the ECJ has started to act as quasi-constitutional court.[76] The Charter has become the parameter to assess the validity and interpret European legal instruments suffering the legislative inertia of the European lawmaker in relation to the challenges of the digital age. This proactive approach has led to shifting from a formal dimension to a substantial application of fundamental rights, or constitutional law in action. Nevertheless, this activity is not new to the ECJ that, even before the Maastricht Treaty entered into force, had underlined the role of fundamental rights as a limit to fundamental freedoms and common market principles.[77] Precisely, the recognition of fundamental rights as general principles of EU law has opened the doors towards a balancing exercise between fundamentals freedoms and rights, or between the economic and constitutional

[69] Charter (n. 10), Art. 11(1).
[70] Ibid., Art. 7.
[71] Ibid., Art. 8(1).
[72] Ibid., Art. 51.
[73] Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2013) 8 (3) European Constitutional Law Review 375.
[74] Convention (n. 37), Art. 17.
[75] Charter (n. 10), Art. 54.
[76] 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.
[77] 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.

dimension of the Union.[78] And this approach is still in the style of the ECJ as shown by the judicial approaches to the challenges raised by digital technologies.

Therefore, the Charter has arisen as a judicial tool to address digital challenges due to the lack of any intervention from the political power. As demonstrated by the next subsections, the ECJ has adopted a teleological approach to ensure the effective protection of constitutional rights and freedoms in relation to the threats of digital technologies implemented by public actors and private businesses 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 played a primary role to highlight the challenges for fundamental rights in the algorithmic society. This judicial approach has promoted the transition from a mere economic perspective towards a reframing of constitutional rights and democratic values defining a new phase characterising European digital constitutionalism.

2.3.1 The Constitutional Dimension of Online Intermediaries

The role of fundamental rights and democratic values is hidden between the lines of the system of content. Apart from the reference to Article 10 of the Convention, there are no other points in the e-Commerce Directive expressing the relationship between online intermediaries and fundamental rights. This gap was evident in the case law of the ECJ before the adoption of the Lisbon Treaty.

In *Google France*,[79] 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 the Advocate General Poiares Maduro, search engine results are a 'product of

[78] 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).

[79] 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.

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'.[80] Likewise, although the ECJ recognised that Google established 'the order of display according to, inter alia, the remuneration paid by the advertisers',[81] this situation does not deprive the search engine from the exemption of liability established by the e-Commerce Directive.[82] Although neither the Advocate General nor the ECJ did recognise the active role of this provider, 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*.[83] 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.[84] 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.

Still, both decisions are the results of a judicial frame based on the economic imprinting of the Union. The predominance of the economic narrative in the judicial reasoning of the ECJ was also the result of the lack of European constitutional parameters to assess the impact on fundamental rights and freedoms. It is not by chance that, after the adoption of the Lisbon Treaty, the ECJ changed its judicial approach moving from a merely economic perspective to a fundamental rights-based approach.

The adoption of a constitutional interpretative angle came up when addressing two cases involving online intermediaries and, primarily, the extent of the ban on general monitoring. In *Scarlet* and *Netlog*,[85] the

[80] Opinion of Advocate General Poiares Maduro in the case *Google France* C-236/08, 144.
[81] Cases C-236/08, C-237/08 and C-238/08 (n. 79), 115.
[82] Ibid., 116.
[83] Case 324/09, *L'Oréal SA and Others* v. *eBay International AG and Others* (2011) ECR I-06011.
[84] Ibid., 116.
[85] 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 and Frederik

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 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.[86] 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.[87] 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 *McFadden*,[88] the ECJ addressed two similar cases involving injunction orders on online intermediaries which left the provider free to choose the measures to tackle copyright infringements while maintaining the exemption of liability by requiring a duty of care in respect of European fundamental rights. The ECJ upheld the interpretation of the referring national court on the same (constitutional) basis argued in *Scarlet* and

Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34(11) European Intellectual Property Review 791.

[86] Case C-70/10 (n. 85), 50.

[87] Charter (n. 10), Arts. 8, 11.

[88] Case C-314/12, *UPC Telekabel Wien GmbH* v. *Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* (2014); Case C-484/14, *Tobias McFadden* 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.

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 safeguards to the digital environment underlining how the economic frame could not be considered enough to address new digital challenges. Even more recently, as examined in Chapter 5, the ECJ has interpreted the framework of the e-Commerce Directive in *Eva Glawischnig-Piesczek*, defining additional safeguards in the removal of identical and equivalent content.[89]

Besides, the ECJ has not been the only European court to stress the relevance of fundamental rights in the field of content. The Strasbourg Court also underlined how the activities of online intermediaries involve fundamental rights. The Court has repeatedly addressed national measures involving the responsibility of online intermediaries for hosting unlawful content such as defamatory comments.[90] Precisely, the Court has highlighted the potential chilling effect on freedom of expression online resulting from holding platforms liable in relation to third-party conduct.[91]

Despite these judicial efforts, the challenges raised by online platforms are far from being solved. European courts have extensively addressed the problem of enforcement in the digital age.[92] Still, the challenge of content moderation raises constitutional concerns. The increasing active role of online platforms in content moderation questions not only the liability regime of the e-Commerce Directive but also constitutional values such as the protection of fundamental rights and the rule of law. Nonetheless, the ECJ's approach has played a crucial part in defining the role of constitutional values in the field of content, driving the evolution of European digital constitutionalism. As underlined in the next sections, the Union has adopted a constitutional strategy in the field of content by orienting its approach towards the introduction of transparency and accountability safeguards in content moderation.

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

[90] See *Delfi AS* v. *Estonia*, Judgment (2015); *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt* v. *Hungary*, Judgment (2016); *Rolf Anders Daniel Pihl* v. *Sweden*, Judgment (2017).

[91] Robert Spano, 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665.

[92] Martin Husovec, *Injunctions against Intermediaries in the European Union. Accountable but Not Liable?* (Cambridge University Press 2017).

2.3.2 The Judicial Path towards Digital Privacy

The role of the ECJ in these cases provides some clues about the role of judicial activism in adjusting constitutional values to a different technological environment and answering the legislative inertia of the European lawmaker. In the field of data, the ECJ has not only focused on underlining the relevance of fundamental rights 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 digital age have encouraged the ECJ to overcome the economic-functional dimension of the Data Protection Directive to a constitutional approach.

As a first step, in *Lindqvist*,[94] the ECJ highlighted the potential clash between internal market goals and fundamental rights. The objectives of harmonising national rules including the free flow of data across Member States can clash with the safeguarding of constitutional values.[95] Precisely, the court underlined how the case in question required to strike a fair balance between conflicting rights, especially the right to freedom of expression and privacy.[96] However, in this case, the judicial focus was still on the right to privacy. Some years later, in *Promusicae*,[97] the ECJ enlarged its view to the right to data protection. In a case involving the scope of a judicial order to disclose the identities and physical addresses of certain persons whom it provided with Internet access services, the ECJ recognised the role of data protection 'namely the right that guarantees protection of personal data and hence of private life',[98] despite its functional link with the protection of privacy.[99]

[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).
[94] Case C-101/01, *Lindqvist* (2003) ECR I-2971.
[95] Ibid., 79–81.
[96] Ibid., 86.
[97] Case C-275/06, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU* (2008) ECR I-271, 63.
[98] Ibid., 63.
[99] 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.

This scenario changed with the entry into force of the Lisbon Treaty. Thereafter, the ECJ has started to apply the Charter to assess the threats to privacy and data protection. Unlike the field of content, the Charter has introduced a new fundamental right consisting of the right to protection of personal data.[100] Therefore, the ECJ has not just framed the scope of application of the right to privacy online, but it has played a crucial role in consolidating the constitutional dimension of data protection within the European context.

The mix of this constitutional addition together with the challenges of the information society has led the ECJ to invalidate the Data Retention Directive,[101] due to its disproportionate effects over fundamental rights. In *Digital Rights Ireland*,[102] 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 proved to be aware of the risks for the protection of the fundamental rights of European citizens. 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'.[103] Moreover, with regard to automated technologies, the ECJ observed that '[t]he need for such safeguards is all the greater where ... personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data'.[104] The influence of this approach can also be examined in further decisions of the ECJ on data retention and, precisely in *Tele 2* and *La Quadrature du Net*.[105]

The same constitutional approach can be appreciated in *Schrems*,[106] where the ECJ invalidated the safe harbour decision, which was the

[100] Charter (n. 10), Art. 8.

[101] 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.

[102] 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). See Federico Fabbrini, 'The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal 65.

[103] Cases C-293/12 and C-594/12 (n. 102), 56.

[104] Ibid., 55.

[105] Case 203/15, *Tele2 Sverige AB contro Post- och telestyrelsen e Secretary of State for the Home Department* v. *Tom Watson e a.* (2016); C-511/18, *La Quadrature du Net and Others* v. *Premier ministre and Others* (2020).

[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 ...

legal basis allowing the transfer of data from the EU to the United States.[107] Also in this case, the ECJ provided an extensive interpretation of the fundamental right to data protection when reviewing the regime of data transfers 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 also in the second decision involving the transfer of personal data to the United States. As examined in Chapter 7, 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 the 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

A Critical View of the Schrems Judgment in the Context of European Constitutionalism' (2017) 16 Global Community Yearbook of International Law and Jurisprudence 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.

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 the ECJ recognised that a search engine like Google falls under the category of 'data controller' shows the predominant role of privacy and data protection as fundamental rights. When interpreting the scope of application of the Data Protection Directive, the ECJ observed that not only a literal but also teleological interpretation, which looks at the need to ensure the effective and complete protection of data subjects, would lead to considering search engines as data controllers 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 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 towards 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 are 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 the removal of the content at stake.[117] As a result, it is possible to argue that this interpretation just unveiled an existing legal basis in the Data Protection Directive to enforce this right against private actors.

[114] Ibid., 34.
[115] Ibid., 58.
[116] Ibid., 60.
[117] Ibid., 97.

https://doi.org/10.1017/9781009071215.003 Published online by Cambridge University Press

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 horizontal enforcement of the fundamental rights enshrined in the Charter. In this way, as also addressed in Chapter 3, 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 demonstrates how the GDPR, as one of the expressions of European digital constitutionalism, has led to the codification of these judicial steps and provided a new harmonised framework of European data protection law.

2.4 The Reaction of European Digital Constitutionalism

The changing landscape of the digital environment has led the ECJ to take the initiative, thus overcoming the inertia of political power. The ECJ's judicial activism has paved the way for a shift from the first approach based on digital liberalism to a new phase of digital constitutionalism characterised by the reframing of fundamental rights and the injection of democratic values in the digital environment.

This change of paradigm does not only concern the power exercised by public actors. As underlined in Chapter 1, public actors are still a primary source of concern but are no longer the only source of interference with individual fundamental rights and freedoms. Threats to constitutional values also come from transnational private actors, precisely online platforms such as social media and search engines whose freedoms are increasingly turning into forms of

[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.

unaccountable power. While constitutional safeguards bind the public sector, these do not generally extend to private actors. Given the lack of regulation or horizontal translation of constitutional values, constitutional law does not limit the freedom which private entities enjoy in performing their activities.

The constitutional gap between the exercise of power by public and private actors has led the Union to abandon the phase of digital liberalism and face new private forms of authority based on the exploitation of algorithmic technologies for processing content and data on a global scale.[119] As also supported by judicial activism, this reaction is not only linked to the protection of individual fundamental rights, such as freedom of expression and data protection, and, at the end, dignity.[120] Even more importantly, the consolidation of private powers raises concerns for the democratic system and, primarily, the principle of rule of law due to the increasing competition between public and private values.[121]

Within this framework, two primary drivers have characterised the rise of the democratic phase of European digital constitutionalism. Firstly, the Union codified some of the ECJ's judicial lessons. Secondly, the Union introduced new limits to private powers by adopting legal instruments by increasing 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] This is because the role of online platforms in the digital environment implies 'wider responsibility'.[124]

[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.

Likewise, the Council of Europe has contributed to the reaction of the Union against the power of online platforms. Particularly, it underlined the relevance of the positive obligation of Member States to ensure the respect of human rights and the role and responsibility of online intermediaries in managing content and processing data. 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'.[125] Even the European Parliament proposed to clarify the boundaries of online intermediaries' liability and to provide more guidance defining their responsibilities.[126]

This political approach resulted in a new wave of soft-law and hard-law instruments whose objective is, inter alia, to mitigate online platform powers in the field of content and data. Like other fields such as net neutrality or the right to Internet access, the introduction of new safeguards constitutes the expressions of key values of the contemporary society.[127] Precisely, the Directive on copyright in the DSM (Copyright Directive),[128] the amendments to the audiovisual media services Directive (AVMS Directive),[129] the regulation to address online terrorist content (TERREG),[130] or the adoption of the GDPR are just some of the examples demonstrating how the Digital Single Market strategy has constituted a change of paradigm to face the consolidation of powers in the algorithmic society. The proposal for the Digital Services Act can be seen as a milestone of this

[125] Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries CM/Rec(2018)2, 7.

[126] European Parliament resolution of 15 June 2017 on online platforms and the digital single market, 2016/2276(INI).

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

[128] 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.

[129] 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.

[130] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (2021) OJ L 172/79.

path,[131] as discussed in Chapter 5. The next subsections examine how the Union has built a constitutional strategy to protect rights and limit powers by introducing obligations and safeguards in the field of content and data.

2.4.1 Democratising Content Moderation

Within the framework of the Digital Single Market strategy, the Commission oriented the efforts towards fostering transparency and accountability in the field of content. To reduce the discretion of online platforms to organise and remove content, the Commission adopted a siloed approach defining new procedural safeguards in different sectors like copyright or audiovisual content.

For the first time after twenty years, the adoption of the Copyright Directive has changed the system of liability established by the e-Commerce Directive but applying only to some online platforms (i.e. online content-sharing service providers) and limited to the field of copyright.[132] Despite this scope, this step can be considered a watershed in the European policy, acknowledging that the activities of some online platforms cannot be considered passive any longer. The digital environment has gained in complexity. The services offered by platforms, particularly social media, allow access to a large amount of copyright-protected content uploaded by their users.[133]

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

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

[132] 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).

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

https://doi.org/10.1017/9781009071215.003 Published online by Cambridge University Press

system between online platforms and rightholders.[134] 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 licences from rightholders. 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 copyright-protected works unless they comply with the new conditions defining the exemption of liability focused on the notion of best efforts.[135]

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'.[136] 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.[137] Furthermore, the Copyright Directive extends the ban on general monitoring not only to Member States but also the cooperation between rightholders and online platforms.[138]

In this case, it is possible to observe the heritage of the ECJ rulings in terms of proportionality safeguards 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 aims to strike a fair balance between the interests of rightholders, the protection of users' rights and the freedom to conduct business, especially concerning small platforms.

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 limited platform powers by introducing procedural safeguards in content moderation. Firstly, the Copyright 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

[134] Copyright Directive (n. 128), Art. 2(6).
[135] Ibid., Art. 17.
[136] Ibid., Art. 17(5).
[137] Ibid., Art. 17(6).
[138] Ibid., Art. 17(8).

on the use of content covered by the agreements.[139] 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.[140] 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.[141] 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.[142] 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 underlines how, on the one hand, the Union has 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 for copyright-protected content. Likewise, the amendment to the AVMS Directive aims to increase the responsibilities of video-sharing platforms.[143] Unlike the Copyright Directive, the AVMS Directive specifies that video-sharing platforms' liability is subject to the provisions of the e-Commerce Directive.[144] 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.[145]

[139] Ibid.
[140] Ibid., Art. 17(9).
[141] Ibid.
[142] Ibid.
[143] AVMS Directive (n. 129), Art. 1(1)(b).
[144] Ibid., Art. 28a(1).
[145] Ibid., Art. 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

https://doi.org/10.1017/9781009071215.003 Published online by Cambridge University Press

Such appropriate measures should also regard audiovisual commercial 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'.[146] 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.[147] Precisely, the nature of the content, the possible harm which it 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 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

racism and xenophobia within the meaning of Art. 1 of Framework Decision 2008/913/JHA.

[146] 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.

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

considered so much as passive providers but as market players whose activities should be subject to regulation.

Similar observations apply to the TERREG which aims to establish a clear and harmonised legal framework to address the misuse of hosting services for the dissemination of terrorist content.[148] Firstly, the TERREG defines terrorist content.[149] 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.[150]

Despite the relevance of these obligations, the implementation of these measures, described as 'duties of care',[151] 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 TERREG 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, they are obliged to remove content within one hour of the receipt of a removal order from the competent authority.[152]

Although the TERREG has raised several concerns since the launch of the first proposal,[153] even in this case, the Union has injected procedural

[148] 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) www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf accessed 21 November 2021; 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 accessed 21 November 2021.

[149] TERREG (n. 148), Art. 2(1)(7).

[150] Ibid., Art. 5.

[151] Ibid., Art. 1(1)(a).

[152] Ibid., Art. 3.

[153] Jillian C. York and Christoph Schmon, 'The EU Online Terrorism Regulation: A Bad Deal' EFF (7 April 2021) www.eff.org/it/deeplinks/2021/04/eu-online-terrorism-regulation-bad-deal accessed 21 November 2021. See, also, FRA, 'Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications. Opinion of the European Union Agency for Fundamental Right' (12 February 2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf accessed 21 November 2021.

safeguards. 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.[154] Furthermore, competent authorities shall make publicly available annual transparency reports on the removal of terrorist content.[155] 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).[156] Furthermore, the TERREG 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.[157] As in the case of transparency obligations, this process aims to regulate content moderation. 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.[158] This process is not entirely discretionary. Within two weeks from the receipt of the complaint, online platforms do not only inform the notice provider but also provide an explanation when they decide not to reinstate the content.

These measures deserve to be framed within the attempts of the Commission to nudge online platforms to introduce transparency and accountability mechanisms.[159] The Recommendation on measures to effectively tackle illegal content online proposes a general framework of safeguards in content moderation.[160] This instrument encourages platforms to publish, in a clear, easily understandable and sufficiently detailed manner, the criteria according to which they manage the

[154] Ibid., Art. 7.
[155] Ibid., Art. 8.
[156] Ibid., Art. 5(2).
[157] Ibid., Art. 10.
[158] Ibid., Art. 10(2).
[159] Code of conduct on countering illegal hate speech online (2016) http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300 accessed 21 November 2021; Code of practice on disinformation (2018) https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation accessed 21 November 2021; 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.
[160] Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C(18) 1177 final.

removal of or blocking of access to online content.[161] 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.[162] 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 aims to reduce the asymmetry between individuals and private actors implementing automated technologies.

Although the European constitutional framework has made some important steps forward in the field of content, however, the legal fragmentation of guarantees and remedies at supranational level could undermine the attempt of the Union to provide a common framework to address the cross-border challenges raised by online platforms. Instead, the Union does not seem to adopt a common strategy in this field but regulates platform by siloes. This situation also raises challenges at the national level as underlined by the implementation of the new licensing system introduced by the Copyright Directive.[163]

Despite the steps 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 laws introduced by Germany in the field of hate speech,[164] and France concerning disinformation.[165] The mix of supranational and national initiatives leads to a decrease in the effective degree of protection of fundamental freedoms and rights in the internal market, thus challenging the role of digital constitutionalism in protecting individual fundamental rights and limiting the powers of online platforms.

[161] Ibid., 16.
[162] Ibid., 9.
[163] 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.
[164] Netzdurchsetzunggesetz, Law of 30 June 2017 (NetzDG).
[165] 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.

Therefore, as examined in Chapter 5, the advent of the Digital Services Act provides a common and horizontal framework supporting the increase of transparency and accountability of content moderation.

2.4.2 Centring a Personal Data Risk-Based Approach

The protection of personal data has reached a new step of consolidation not only after the adoption of the Lisbon Treaty thanks to the role of the ECJ but also with the adoption of the GDPR. The change in the strategy of the Union can be examined 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.[166] This focus on fundamental rights does not 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 by promoting innovation within the context of the data industry.[167] However, this change of paradigm in the approach of the Union underlines a commitment to protect fundamental rights and democratic values in the algorithmic society.

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 to the system of data protection law.[168] Even when the data controller is not established in the Union,[169] 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.[170] In other words, even in this field, the approach of the Union aims to move from formal compliance as a legal shield to substantive

[166] GDPR (n. 56), Recitals 1–2.
[167] Ibid., Recital 4.
[168] Ibid., Art. 5.
[169] Ibid., Art. 3(2).
[170] 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' (2017) 8(3) European Journal of Risk Regulation 506.

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 influence of the ECJ's lessons can be read by examining how the GDPR aims to overcome formal approaches (e.g. establishment) and adopt a risk-based approach to preclude data controllers from escaping 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 individual 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's principles.[171] The principle of accountability can be considered a paradigmatic example of how the Union aims to inject proportionality in the field of data.

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.[172] 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'.[173] 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 increased the degree of accountability of the data controller but also has also aimed to empower individuals by introducing new rights for data subjects. The case of the right to erasure can be considered a paradigmatic example of the codification

[171] Ibid., Art. 24.
[172] Ibid., Art. 25.
[173] Ibid., Art. 35(3)(a).

https://doi.org/10.1017/9781009071215.003 Published online by Cambridge University Press

process in the aftermath of the ECJ's case law, precisely *Google Spain*.[174] The right not to be subject to automated decisions and the right to data portability are only two examples of the new rights upon which users can rely.[175] In other words, the provisions of new data subjects' rights demonstrate how the Union intends to ensure that individuals are not marginalised vis-à-vis the data controller, especially when the latter processes 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, the GDPR provides a general rule, according to which, subject to some exceptions,[176] 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 analysed in Chapter 6, despite this vague scope of this right which tries to provide a flexible approach to different automated decision-making systems, the GDPR aims to protect data subjects against this form of automated processing. 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, the GDPR aims to ensure not only the right to privacy and data protection but also individual autonomy and dignity.[177] 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 their rights and freedoms.

However, that enhancing procedural safeguards could affect the freedom to conduct business or the performance of a public task due to additional human and financial resources required to adapt automated technologies to the data protection legal framework. More broadly, this situation could also contribute to the consolidation of existing platform

[174] Jef Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press 2020).
[175] GDPR (n. 56), Arts. 20, 22.
[176] Ibid., Art. 22(2).
[177] Ibid., Art. 22(3).

powers creating a legal barrier for other businesses to use these technologies.[178] Secondly, the presence of a human being does not eliminate any risk of error or discrimination, especially considering that, in some cases, algorithmic biases are the results of data collected by humans or reflecting human prejudices.[179] Thirdly, the opacity of some algorithmic processes could not allow the data controller to provide the same degree of explanation in any case. This point is primarily connected to the debate around the right to explanation in European data protection law.[180]

Nevertheless, this provision, together with the principle of accountability, constitutes a crucial step in the governance of automated decision-making processes.[181] 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, the principle of the rule of law since, even in this case, legal norms are potentially replaced by technological standard and private determinations 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.[182] The potential scope of the principle of accountability leaves data controllers to enjoy margins of discretions in deciding the safeguards that are

[178] Michal S Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) Journal of Competition Law and Economics 349.

[179] Andreas Tsamados and others. 'The Ethics of Algorithms: Key Problems and Solutions' (2021) AI & Society https://link.springer.com/article/10.1007/s00146-021-01154-8#citeas accessed 21 November 2021.

[180] 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 Berkeley 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.

[181] Margot Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529.

[182] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250.

enough to protect the fundamental rights of data subjects in a specific context. As underlined in Chapter 3, 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.

2.5 Freedoms and Powers in the Algorithmic Society

The advent of the Internet 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 considered 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 humus of European constitutional values. This transatlantic distance underlines why the first phase of digital liberalism was destined to fall before the rise of new private actors interfering with individual 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 last century. Nonetheless, the new European approach to the challenges of the algorithmic society 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 internal market, the Union's approach moved to a constitutional-based approach. The ECJ has played a crucial role in this transition by building a constitutional bridge allowing the Union to move from digital liberalism to a democratic constitutional strategy. The Commission then codified and consolidated this shift as demonstrated by the approach taken with the Digital Single Market Strategy.

The rise of European digital constitutionalism can be considered a reaction against the challenges of the algorithmic society, and in particular the rise of platform powers. The liberal approach adopted by constitutional democracies recognising broad areas of freedom both in the field of content and data has led to the development of business models providing opportunities for fundamental rights and freedoms online. At the same time, the price to pay for leaving broad margin of freedoms to the private sector has contributed to turning freedoms into powers. In other words, the digital liberal approach of the Union has promoted the rise and consolidation of private ordering competing with public powers.

As analysed in Chapter 3, technological evolutions, combined with a liberal constitutional approach, have led online platforms to exercise delegated and autonomous powers to set their rules and procedures on a global scale. Therefore, users are subject to 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 underlined in the next chapter, the powers exercised by online platforms, as transnational private actors, have raised constitutional challenges which still need to be addressed.