7 The Road Ahead of European Digital Constitutionalism

7.1 The Consolidation of European Digital Constitutionalism

The European path towards digital constitutionalism has led to a shift of paradigm. The liberal goals of the internal market have met democratic values, thus building a new (digital) constitutional approach. As examined in Chapter 2, European constitutional values have enriched the digital liberal approach adopted at the end of the last century, which has been slowly complemented by a democratic strategy. This shift has been possible thanks to the consolidation of the European constitutional order in the aftermath of the Lisbon Treaty and the ECJ's judicial lessons, which have paved the way towards the constitutional reaction characterising the third (constitutional) phase opposing the troubling rise and evolution of private powers in the algorithmic society.

At the dawn of a new digital constitutional phase in Europe, it is worth wondering in which direction the Union will orient its strategy in the fourth revolution.[1] The Union has already demonstrated its commitment to be an active part of global dynamics of the digital age.[2] In her political guidelines, Commission president von der Leyen underlined the two political branches guiding the Union in the next decades to ensure the transition to a healthy planet and a new digital world which are

[1] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2020. A Union that strives for more, COM(2020) 37 final.

considered as complementary areas.[3] The mix between environment and technology is critical,[4] as also highlighted by the UN Sustainable Development Goals.[5] The Data Strategy aims to establish the creation of a 'single European data space'.[6] It consists of ten sectoral common European data spaces which are relevant for the twin purposes of green and digital transitions. Shaping the digital future is based on the balancing between the interests in ensuring innovation in the internal market and protecting fundamental rights and democratic values.[7] The Data Governance Act is a leading example of this approach.[8] Likewise, the White paper on artificial intelligence is another piece of the European constitutional strategy,[9] as then translated in the proposal for the Artificial Intelligence Act.[10]

The focus on the digital future of the Union fits exactly within the global rush to build a position of standard maker in the algorithmic society. China is approaching being the world leader in the field of artificial intelligence technologies by 2030.[11] Whereas the US tech giants dominate digital markets and continue to extend their power to other sectors.[12] The role of digital technologies, particularly artificial intelligence, for the fourth industrial revolution does not only relate to

[3] Luciano Floridi, 'The Green and the Blue: Naïve Ideas to Improve Politics in a Mature Information Society' in Carl Öhman and David Watson, *The 2018 Yearbook of the Digital Ethics Lab* 183 (Springer 2018).

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal, COM(2019) 640 final.

[5] UN General Assembly, Resolution adopted by the General Assembly on 25 September 2015 A/RES/70/1 (2015).

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data, COM(2020) 66 final.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67 final.

[8] Proposal for a Regulation of the European Parliament and of the Council on European Data Governance COM(2020) 767 final.

[9] White paper, 'On Artificial Intelligence – A European Approach to Excellence and Trust' COM(2020) 65 final.

[10] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM(2021) 206 final.

[11] Will Knight, 'China Plans to Use Artificial Intelligence to Gain Global Economic Dominance by 2030' MIT Technology Review (21 July 2017) www.technologyreview.com/2017/07/21/150379/china-plans-to-use-artificial-intelligence-to-gain-global-economic-dominance-by-2030/ accessed 21 November 2021.

[12] Nick Srnicek, *Platforms Capitalism* (Polity Press 2016).

the potentialities of these technologies but also to their dissemination in the society and to commodification.[13] These technologies are no longer closed to the domain of academics or specific business sectors, but are spreading in daily lives, gathering data and information, which then contribute to training artificial intelligence technologies promising new opportunities based on predictive models and answers.[14] This process could play a critical role for the expansion of the internal market and in keeping it competitive in the international arena. At the same time, if, on the one hand, artificial intelligence is likely to provide new opportunities for the Union and Member States, on the other hand, they also pose relevant challenges for society,[15] especially concerning fundamental rights and democratic values.[16]

The previous chapters have underlined how the evolution of the digital environment have led constitutional democracies to adopting a liberal approach to protect innovation, thus leading to the rise of new digital powers. Against these challenges, the rise of digital constitutionalism has provided a first reaction laying the foundations to build a European strategy in the next years to avoid constitutional values slowly fading away in the name of innovation or business purposes outside democratic channels. However, as stressed in Chapters 5 and 6, the path has just started. The Digital Services Act and the GDPR have been just the first answers of the European constitutional strategy in the field of content and data.[17] This is why the rise of digital constitutionalism looks far from being

[13] Brandon Allgood, 'The Commoditization of AI and The Long-Term Value of Data' Forbes (10 April 2017) www.forbes.com/sites/forbestechcouncil/2017/04/10/the-commoditization-of-ai-and-the-long-term-value-of-data/#74c71abd159c accessed 21 November 2021.

[14] Brian Cantwell Smit, *The Promise of Artificial Intelligence. Reckoning and Judgment* (MIT Press 2019).

[15] Sue Newell and Marco Marabelli, 'Strategic Opportunities (and Challenges) of Algorithmic Decision-making: A Call for Action on The Long-Term Societal Effects of 'Datification' (2015) 24 The Journal of Strategic Information Systems 3.

[16] Mireille Hildebrandt, 'The Artificial Intelligence of European Union Law' (2020) 21 German Law Journal 74; Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2020) 376 Philosophical Transaction A.

[17] 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; 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.

a point of arrival or the last step of the European constitutional path in the algorithmic society.

It is already possible to examine some trends leading the European constitutional strategy before dilemmas or trade-offs which could lead to polarisation. Firstly, automated decision-making technologies developed by transnational actors are promising new opportunities for growth and innovation. Like at the end of the last century, this promising scenario could trigger neoliberal approaches, thus contributing to the the path of digital capitalism. At the same time, these technologies have already highlighted the challenges for the protection of fundamental rights and freedoms, thus raising questions about safeguarding human dignity. Therefore, the first dilemma is a matter of values driving the algorithmic society (i.e. digital humanism versus digital capitalism).

Secondly, it is worth focusing on the governance of these values. The mix of public authority and private ordering contributes to shaping the evolution and implementation of digital technologies. Both public and private powers propose models for governing technology which do not always lead to cooperation but sometimes also to competition, thus blurring the boundaries between different normativities. The dilemma between hard- and self-regulation is one of the primary challenges for constitutional democracies which are still following diverging strategies in the algorithmic society (i.e. public authority versus private ordering).

Thirdly, the global spread of algorithmic technologies leads to focusing on the scope of these values and their governance at the intersection between public and private actors. While the traditional characteristics of sovereign powers would limit the application of rights and freedoms to a certain territory, private actors enjoy more flexibility in extending their standards on a global scale. As a result, public actors are encouraged to make the protection of fundamental rights extraterritorial to mitigate the influence of global standards developed by unaccountable private entities or other external interferences by other states. At the same time, the limits to the exercise of sovereign powers beyond territorial boundaries could encourage constitutional democracies to look at global phenomena with scepticism while fearing the consequences of reciprocity. Illiberal regimes could take the extraterritorial application of rights and freedoms as a model to support the extension of their illiberal agenda beyond their boundaries. This trend could trigger a protectionist reaction by constitutional democracies to shield constitutional values from the

interferences of global private standards and illiberal public values (i.e., constitutional imperialism versus constitutional protectionism).[18]

Within this framework, this chapter argues that the characteristics of European digital constitutionalism defines a third way escaping polarisation. The primary goal of this chapter is to underline how the talent of European digital constitutionalism promotes a sustainable growth of the internal market and the protection of fundamental rights and democratic values in the long run. The first part of this chapter focuses on the relationship between digital humanism and digital capitalism underlining the potential path characterising the European approach to artificial intelligence technologies. The second part examines how European digital constitutionalism would lead to a third way between public authority and private ordering. The third part underlines to what extent the Union would likely extend the scope of its constitutional values to address the global challenges of artificial intelligence technologies. Once this chapter addresses the potential road ahead of European digital constitutionalism, the fourth part summarises the primary findings of this research.

7.2 Values: Digital Humanism versus Digital Capitalism

The development of artificial intelligence technologies has triggered a new wave of opportunities for economic growth. The processing of vast amounts of data have become an integral part of the public and private sector. While, in the last century, the lack of a vast amount of interconnected data has led to the so-called AI winters,[19] today, the evolution of global communication technologies allowing the storing and exchange of information seems to promise a different path.

The availability of large data sets has led to a sharp increase in the number of intelligent products and services. Although most of the automated systems are still in the phase of 'narrow AI', significant improvements have been achieved, for example, in the analysis and prediction of human behaviour and characteristics, or in the field of

[18] James Tully, 'The Imperialism of Modern Constitutional Democracy' in Martin Loughlin and Neil Walker (eds.), *The Paradox of Constitutionalism: Constituent Power and Constitutional Form* (Oxford University Press 2008).

[19] Luciano Floridi, 'AI and Its New Winter: From Myths to Realities' (2020) 33 Philosophy & Technology 1.

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

robotics.[20] From banking and insurance to the medical sector, automated decision-making technologies offer new possibilities of prediction and interpretation of reality based on different degrees of determinism like neural networks. One example consists of biometric technologies where voice and facial recognition are not only implemented by public authorities for the performance of public tasks like border control,[21] but also by the private sector, primarily to profile individuals for business purposes.[22]

This is why artificial intelligence is one of the primary drivers of the fourth industrial revolution. Data are the fundamental asset for the digital economy due to their capacity to generate value. At the same time, the previous chapters have shown how automated technologies have highly challenged the protection of fundamental rights and democratic values. Discriminatory results, biased decisions, censoring speech or subject users to forms of surveillance are only some examples of these concerns.[23] Health and security, privacy and self-determination, speech and discrimination, are just examples of the values involved in processes of decision-making outside human judgment or oversight. This scenario leads to a crossroads between a model where individual rights and freedoms are shielded against the appeal and promise of new technologies (i.e. digital humanism) and a neoliberal view looking at the new opportunities of artificial intelligence technologies as a potential engine for economic growth and individual autonomy (i.e. digital capitalism).

This would not be the first time that constitutional democracies face this dilemma. Turning back and looking at the last twenty years, the Union has already addressed this question moving from a digital liberal approach coming from the US neoliberal paradigm to a constitutional approach which takes into high consideration the protection of fundamental rights and democratic values in the algorithmic society. At the end of the last century, there were not so

[20] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 UC Davis Law Review 399.

[21] Paul De Hert, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Patrizio Campisi (ed.), *Security and Privacy in Biometrics* 369 (Springer 2013).

[22] Lauren Stewart, 'Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security' (2019) 60 Boston College Law Review 347.

[23] David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Polity Press 2018).

many clues to look at the rise of digital capitalism as a potential challenge for constitutional democracies. Nonetheless, this liberal approach has been exactly the constitutional ground for the evolution of digital powers against which European digital constitutionalism has reacted. Chapters 5 and 6 have underlined the role of European constitutionalism, and precisely human dignity, in promoting new positive approaches in the fields of content and data. The rise of a new phase of digital constitutionalism can be considered a natural European reaction to the threats of digital capitalism.

Therefore, human dignity is increasingly raising as the last resort to mitigate the potential threats of tecno-determinist solutions that could lead to processes of dehumanisation and gradually the vanishing of democratic values. According to the European Data Protection Supervisor, '[The] respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics'.[24] The consolidation of the algorithmic society brings with it ethical and legal concerns like the autonomy of robots, online censorship and trust in automated decision-making processes.[25] Digital ethics is at the centre of the European policy response to the challenges raised by artificial intelligence technologies in terms of liability, safety, the Internet of Things (IoT), robotics, algorithmic awareness, consumer and data protection.

It should not come as a surprise that a human-centred approach is the core of the European strategy to artificial intelligence. In 2018, the Commission appointed a new High-Level Expert Group on Artificial Intelligence which published its artificial intelligence ethical guidelines.[26] The group underlined the importance of adopting a pan-human approach to these technologies which looks at human dignity as the common foundation of European fundamental rights and values according to which 'the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields'.[27]

[24] European Data Protection Supervisor, 'Opinion 4/2015. Towards a new Digital Ethics' (11 September 2015) https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf accessed 21 November 2021.

[25] Mark Coeckelbergh, *AI Ethics* (MIT Press 2020); Michael Kearns and Aaron Roth, *The Ethical Algorithm: The Science of Socially Aware Algorithm Design* (Oxford University Press 2019).

[26] High-Level Expert Group, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 accessed 21 November 2021.

[27] Ibid., 10.

The same approach is also reflected in the strategy of the Union on artificial intelligence.[28] The white paper on artificial intelligence expressly clarifies that '[g]iven the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'.[29] The Council of Europe also underlined to be aware of the positive and negative impact that the application of algorithmic systems 'has on the exercise, enjoyment and protection of all human rights and fundamental freedoms, and of the significant challenges, also for democratic societies and the rule of law, attached to the increasing reliance on algorithmic systems in everyday life'.[30]

From this perspective, the Union seems to define a precise path towards digital humanism. A closer look can reveal how the Union has not entirely closed its doors to digital capitalism. It is true that protecting rights and democratic values against a reckless race to innovation towards dehumanisation is one of the aims of European digital constitutionalism. Nonetheless, the situation is more nuanced than it could appear at first glance. The European constitutional safeguards could be considered as limits to the development of digital technologies and, therefore, be a competitive disadvantage vis-à-vis other global technological poles, like China or the US.

As examined in Chapter 5, the Union has adopted a more restrictive approach to the power of online platforms over content. Precisely, the European strategy has focused on shaping the boundaries of online platform responsibilities in Europe. A first positive reaction of the Union has led to remedying the discretionary interferences coming from platform power by introducing transparency and accountability safeguards in content moderation. Likewise, Chapter 6 has underlined the role of data protection in counterbalancing and preventing disproportionate interferences with individual personal data and, therefore, autonomy and dignity. In this sense, the GDPR can be considered as the horizontal translation of a mix of constitutional values characterising European constitutionalism.

[28] COM(2020) 65 (n. 9).
[29] Ibid., 2.
[30] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (8 April 2020) www.statewatch.org/media/documents/news/2020/apr/coe-recommendation-algorithms-automation-human-rights-4–20.pdf%3E"www.statewatch.org/media/documents/news/2020/apr/coe-recommendation-algorithms-automation-human-rights-4–20.pdf%3E accessed 21 November 2021.

These limits to safeguard fundamental rights and democratic values would not raise concerns if the Union was the only actor participating in the run towards artificial intelligence technologies around the world. Even if these safeguards aim to protect constitutional values, they could also slow down the smooth development of digital technologies. Granting extensive protection to fundamental rights over innovation could lead the Union to become a 'standard-taker' rather than a 'standard-maker' in the fourth industrial revolution. It would be enough to focus the broad constitutional protection recognised to personal data in the European context to argue, at least apparently, a competitive disadvantage of the Union vis-à-vis other countries where the safeguards in the field of content and data are not equivalent. Since granting 'extensive protection of data privacy rights restrains the use of AI's most useful features: autonomy and automation',[31] one of the most important challenges for the Union in the fourth industrial revolution is to understand where to draw a line between innovation and risk.

Considering the role of artificial intelligence for the fourth industrial revolution, this is not a trivial constitutional issue. A lower degree of guarantees and safeguards can constitute a competitive advantage in the algorithmic society. This situation could trigger a rush to the bottom in the protection of fundamental rights in order not to suffer a competitive disadvantage. It cannot be excluded that the fight in the international arena for becoming the standard-maker in the field of artificial intelligence could lead to a dangerous reduction in democratic and constitutional safeguards in the name of innovation. The extensive protection of individual fundamental rights and democratic values could lead the Union in a position of technological *subjectionis* driven by the extension of technological paradigms of protection coming from areas of the world which do not ensure adequate safeguards for users and society at large. Put another way, this constitutional disadvantage could lead Europe to dealing with a situation of de facto technological disadvantage compared to areas of the world where the lack of restrictions allow the development of technologies becoming market standards. The need to be competitive in a global market would lead the

[31] Matthew Humerick, 'Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2018) 34 Santa Clara High Technology Law Journal 393, 412.

Union to accepting the extension of external paradigms of protection, thus influencing European values.

Within this multifaceted framework, the primary challenge concerns what kind of innovation the Union wants to achieve and whether this choice is based on a liberal approach reducing the scope of safeguards in the name of innovation. Therefore, the question would be whether, in this bipolar system made of opportunities and threats, European digital constitutionalism could provide a third way precluding neoliberal approaches or illiberal agenda from taking the lead of the algorithmic society.

The position of the Union in this field is peculiar due to the role of the two technological poles, precisely China and the US, which are currently leading the fourth industrial revolution.[32] In this geopolitical scenario, the Union has shown its intent to be a crucial player in this match,[33] as also underlined by the proposal for the Artificial Intelligence Act. Although the Union is aware of the potentialities of these technologies and the need to be competitive in the international arena, the protection of fundamental rights, such as personal data, together with the compelling need to protect democratic values against the threats raised by artificial intelligence technologies could constitute a 'constitutional brake' limiting the flourishing of these technologies.

Despite this consideration, the Union has not totally abandoned its economy roots.[34] It should not come as a surprise if the Union agenda already demonstrated a commitment to build a Digital Single Market.[35] To benefit from the full potentialities of this new technological

[32] Klaus Schwab, *The Fourth Industrial Revolution* (Crown 2016); Daniel Araya, 'Governing The Fourth Industrial Revolution' Forbes (12 May 2019) www.forbes.com/sites/danielaraya/2019/03/12/governing-the-fourth-industrialrevolution/#4eea13a14b33 accessed 21 November 2021.

[33] See, e.g., Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, COM(2018) 237 final; Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence COM(2018) 795 final.

[34] Sophie Robin-Olivier, 'The 'Digital Single Market' and Neoliberalism: Reflections on Net Neutrality' in Margot E. Salomon and Bruno De Witte (eds.), *Legal Trajectories of Neoliberalism: Critical Inquiries on Law in Europe* 45 (RSCAS 2019).

[35] 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.

framework, it is necessary to invest resources and ensure the smooth development of these technologies without hindering innovation. In the mid-term review of the Digital Single Market strategy, the Commission highlighted the relevance of being in a leading position in the development of artificial intelligence technologies.[36] It underlined the importance for the Union to benefit from the opportunities of these technologies through a three-pronged approach: increasing public and private investment; preparing for socio-economic changes brought about by artificial intelligence; and ensuring an appropriate ethical and legal framework.

The Union has underlined its intention not only to limit platform power and mitigate the threats of digital capitalism but also to become a standard-maker rather than a mere follower of other technological poles. The Digital Services Act aims not only to increase responsibilities of online platforms and certainty in the moderation of content but also to ensure fair competition and promote the development of small- and medium-sized businesses.[37] Moving to the field of data, while the GDPR increases the degree of protection for individual fundamental rights, other aspects promote the processing of personal data in the business sector and leave some areas of governance to the private sector. In this case, the GDPR can be considered a regulation of surveillance capitalism which does not impede tech giants to collect and process data but regulates this process.

Likewise, the proposal for the Artificial Intelligence Act could provide an example of this hybrid approach. At first glance, this proposal does not focus on individual protection but provides top-down standards defined by the Commission to mitigate the risk coming from artificial intelligence technologies. In other words, rather than a piece in the puzzle of digital constitutionalism, the proposal looks far from the structure of the GDPR or the Digital Services Act. Nonetheless, the objective of the proposal is not only to promote the development of artificial intelligence technologies in Europe to foster the development of the internal market but also to avoid that misuse of technologies producing risks for public interests and rights that would 'contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection

[36] COM(2018) 237 final (n. 33).
[37] COM(2020) 825 final (n. 17).

and privacy and the rights of the child'.[38] This duality of goals is precisely the characterisation of the European approach at the intersection between digital humanism and digital capitalism.

This mix between innovation and the protection of individual fundamental rights is not just the result of regulatory choices but reflects the characteristics of European constitutionalism where the need to balance different fundamental rights could not lead digital humanism or digital capitalism to entirely prevail over each other. The constitutional protection of freedom of expression, privacy and personal data requires to take into consideration not only how to safeguard fundamental rights but also other conflicting interests such as the freedom to conduct business. At the same time, the freedom to conduct business or the aim to achieve the goals of the internal market cannot lead to the annihilation of fundamental rights and freedoms. European constitutional law is not prone to recognise an absolute protection to constitutional values which would lead to the destruction of other conflicting interests.

Therefore, European digital constitutionalism would lead towards a hybrid approach between digital humanism and capitalism. This European 'third way' should not be considered just a political choice but the result of the natural tendency of European constitutionalism not to take a polarised position but merge the different pieces of the puzzle in a dialectic form. The Union does not aim to leave private actors free to develop technologies under a neoliberal scheme such as in the US or strongly intervene in the market to support the development of new technologies and businesses as is the case of China. As we will underline in the next sections, the Union is rising as a global regulator driven by a balanced constitutional approach whose beacon is represented by the principle of human dignity. This approach belongs to the nature of the Union since it is 'founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'.[39]

In front of the crossroads between digital humanism and capitalism, the Union seems to have chosen a path towards the development of a sustainable artificial intelligence environment rather than focusing just on fostering innovation to exploit the potentialities of these

[38] COM(2021) 206 final (n. 10), Recital 15.
[39] Consolidated version of the Treaty on European Union (2012) OJ C 326/13, Art. 2.

technologies or merely impeding their development. Although the Union approach could be subject in the short term to a competitive disadvantage in the field of artificial intelligence, in the long term, the European approach could promote a human-centric development of artificial intelligence technologies. As stressed by the Commission, '[g]iven the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'.[40] Put another way, against a fierce global competition in the field of artificial intelligence and considering its relevance for the future of Europe, the Union has chosen to promote the development of these technologies without forgetting the protection of rights and freedoms.

The definition of this European strategy cannot be understood without examining the governance of these values. It is worth wondering how the Union would concretely put in place its strategy at the intersection between digital humanism and digital capitalism. In order to ensure that technology does not order society and human beings, but is functional to the evolution of mankind, it is critical to wonder about the relationship between the exercise of public authority and private ordering, precisely between the role of hard regulation and self-regulation.

Choosing between public authority or private ordering in the algorithmic society is not a neutral choice. As underlined in the previous chapters, the private governance of content and data in the digital environment left individuals at the margins and subject to private ubiquitous systems influencing their decisions without being able to understand or control the technologies and, therefore, to participate consciously in a democratic society. Therefore, the primary challenge is how citizens can ensure that constitutional values underpinning their social contract are not left to unaccountable determinations outside democratic circuits.

This is a question concerning the governance of values in the algorithmic society. As underlined by the Council of Europe, 'ongoing public and private sector initiatives intended to develop ethical guidelines and standards for the design, development and ongoing deployment of algorithmic systems, while constituting a highly welcome recognition of the risks that these systems pose for normative values, do not relieve Council of Europe Member States of their obligations as primary

[40] COM(2020) 65 final (n. 9), 2.

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

guardians of the Convention'.[41] Rather than proposing a self-regulatory approach, the consolidation of European digital constitutionalism would increasingly lead public actors to be gatekeepers of democratic values, thus defining the framework of values guiding the development of artificial intelligence technologies. The next subsection underlines how finding a point of balance between the exercise of public authority and private ordering would be critical to promote a sustainable and democratic development of artificial intelligence technologies in Europe.

7.3 Governance: Public Authority versus Private Ordering

'People are entitled to technology that they can trust. What is illegal offline must also be illegal online. While we cannot predict the future of digital technology, European values and ethical rules and social and environmental norms must apply also in the digital space'.[42] This political statement underlines the importance of the European values in the development of digital technologies. However, defining values is just one step. The positive consequences of the spread of artificial intelligence firmly clashes with the troubling opacity of 'algocracy'.[43] Individuals are increasingly surrounded by ubiquitous systems whose values are governed by public and private actors. Leaving algorithmic technologies without any democratic safeguard would lead to open the way to a form of technodeterminism, allowing not only public authorities but also private actors to govern algorithmic technologies to autonomously determine the standard of protection of rights and freedoms on a global scale. The Council of Europe underlined the importance of 'bearing in mind that digital technologies hold significant potential for socially beneficial innovation and economic development, and that the achievement of these goals must be rooted in the shared values of democratic societies and subject to full democratic participation and oversight'.[44] Therefore, in order to protect democratic values while promoting innovation, defining the governance of artificial

[41] CM/Rec(2020)1 (n. 30).
[42] COM(2020) 67 final (n. 7), 10.
[43] John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 Philosophy & Technology 245.
[44] CM/Rec(2020)1 (n. 30).

intelligence technologies is a critical piece of the puzzle. Put another way, the Union's choice at the intersection between digital humanism and digital capitalism may be effective only if the Union will adopt a system of governance which can ensure the effective implementation of the European democratic approach to the algorithmic society.

As examined in Chapter 3, transnational private actors have consolidated delegated and autonomous areas of powers while privately ordering the fields of content and data. The rise of European digital constitutionalism can also be read as a reaction against the power of online platforms to set their values on a global scale on a discretionary basis. Content moderation and individual profiling are just two examples of how private actors have been able to rely on a self-regulatory framework driven by business logics rather than by public values. While, at the end of the last century, the primary concern was not overwhelming the private sector with regulatory burdens, now, the Union is showing to be concerned about the dramatic shift from public values to private determinations driven by profit maximisation. The rise of digital capitalism is nothing else than the fruit of a digital liberal approach which has not considered how leaving private actors without a framework of safeguards and oversight could affect society at large and lead to a concentration of digital private powers.

The Union has already expressed its commitment not to be subject to the logics of digital capitalism. According to Vestager, 'platforms [. . .] can have an enormous impact on the way we see the world around us. And that's a serious challenge for our democracy. . . . So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms'.[45]

The European orientation to digital ethics underlines that the market cannot autonomously prevail over the need to safeguard fundamental rights and democracy. Ethics could play a critical role in the making of artificial intelligence governance.[46] Nonetheless, an extensive reliance

[45] Margrethe Vestager, 'Algorithms and Democracy' Algorithmic Watch (30 October 2020) https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue-30-october-2020_en accessed 21 November 2021.

[46] Coeckelbergh (n. 25); Virginia Dignum, *Responsible Artificial Intelligence* (Springer 2019); Luciano Floridi and others, 'AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28(4) Minds and Machines 689.

on solutions based on ethics and self-regulation could not solve the current situation of asymmetry of power in the algorithmic society. The predominance of ethics over the law could build a neoliberal narrative diluting the role of regulation over self-regulation, thus leading the private sector to define what is good behaviour or, more precisely, what is an objectionable conduct online. Even if companies share their commitment to ethical values or refer to their responsibilities in relation to human rights, they are still free to establish their business purposes which, in the lack of incentives, are usually not oriented to public interests as much as to profit maximisation.

When looking outside the Union, there are other examples which are trying to govern the values underpinning the evolution of tomorrow's digital environment. In the US, the neoliberal approach in the last twenty years would represent a different form of digital constitutionalism. The executive order on preventing online censorship is an interesting example to understand the characteristics of US digital constitutionalism,[47] even if the order was withdrawn in May 2021,[48] and courts had already blocked users' complaints.[49] The presidential move resulted in a constitutional paradox.[50] Beyond the constitutional issues involving the separation of powers between the executive and legislative powers, as the former has no power to amend the work of the latter, the order is incoherent when looking at how the First Amendment has protected online intermediaries in the last twenty years,[51] as also demonstrated by the legislative attempts to amend the Communication Decency Act.

[47] Executive Order on Preventing Online Censorship (28 May 2020) www.federalregister.gov/documents/2020/06/02/2020-12030/preventing-online-censorship accessed 21 November 2021.

[48] 'Executive Order on the Revocation of Certain Presidential Actions and Technical Amendment' (14 May 2021) www.whitehouse.gov/briefing-room/presidential-actions/2021/05/14/executive-order-on-the-revocation-of-certain-presidential-actions-and-technical-amendment/ accessed 21 November 2021.

[49] *Gomez* v. *Zuckenburg,* 2020 U.S. Dist. LEXIS 130989 (N.D.N.Y. July 23, 2020).

[50] Giovanni De Gregorio and Roxana Radu, 'Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech' MediaLaws (6 June 2020) www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/ accessed 21 November 2021.

[51] Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power Over Online Speech' (2019) Hoover Institution, Aegis Series Paper No. 1902 www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf accessed 21 November 2021.

Likewise, moving from the legislative to judicial power, the order was also not in line with the recent orientation of the US Supreme Court. Without going into the details of national case law like *Lewis* v. *YouTube*,[52] Chapter 5 has already underlined how the Supreme Court defined social media as the vast democratic forum of the Internet in *Packingham* v. *North Carolina*.[53] The order also refers to *Pruneyard Shopping Center* v. *Robins* to argue that, although social media platforms are private actors, they provide a public forum online. Nonetheless, these cases deal with the banning of national law introducing a prior restraint over free speech.[54] These cases should have been enough to impede the public interferences to free speech that this executive order introduces. Besides, in a 2019 decision, *Manhattan Community Access Corp.* v. *Halleck*,[55] the Supreme Court closed the door to a potential extension of the state action doctrine when it decided that private actors, precisely cable tv companies operating public access channels, do not serve as a public actor (i.e. the city of New York) and are thus not bound to protect free speech rights. The relevance of this decision can be understood when looking at the national case law which has already relied on this decision to ban interference with platform freedoms such as in *PragerU* v. *YouTube*.[56]

This liberal framework characterising US digital constitutionalism will likely constitute the perfect environment for the consolidation of private ordering in the following years. Online platforms have started a process of institutionalisation by attracting legitimation for their functions and proposing alternative models to the traditional exercise of public powers. The Facebook Oversight board is a paradigmatic example of this process. No matter whether it may be considered as independent or as a supreme court, this process shows how platforms enforce human rights standards not only as instrument of scrutiny over the decisions of Facebook based on their community guidelines but also represent a model of private adjudication in the algorithmic society which, de facto, competes with the model of justice and procedures proposed by public authorities.

On the other pole, China is following a different strategy. Rather than adopting a neoliberal approach to the digital environment, China has always exercised sovereign powers over the Internet to control online

[52] *Lewis* v. *YouTube*, 197 Cal. Rptr. 3d 219 (Cal. Ct. App. 2015).
[53] *Packingham* v. *North Carolina*, 582 U.S. ___ (2017).
[54] *Pruneyard Shopping Center* v. *Robins*, 447 U.S. 74 (1980).
[55] *Manhattan Community Access Corp*. v. *Halleck*, No. 17-1702, 587 U.S. ___ (2019).
[56] *Prager University* v. *Google LLC*, No. 18-15712 (9th Cir. 2020).

activities.[57] The case of the social credit system is an example of the control that China can exercise in the algorithmic society.[58] In these years, after firstly excluding other digital companies like US tech giants through the Great Firewall,[59] China has ensured a walled market environment allowing its businesses to grow outside competition under the Huawei model.[60] This approach has led to the creation of a Chinese digital political economy focused on surveillance and market intervention.

Within this framework, the Union is going towards a different path. Rather than adopting a mere neoliberal approach or supporting the development of its model of the Internet, it is emerging at the intersection between the two models. The governance of values in the algortihmic society is not left either to private determinations through self-regulation or market intervention. The Union is consolidating a co-regulatory approach characterised by the definition of the value framework within which the private sector operates. Therefore, European constitutional values are not simply shaped by private determinations or by unaccountable forces, but are protected by a common regulatory framework injecting constitutional values in self-regulation. This result is not by chance but derives from the path of European digital constitutionalism.

Despite its economic history, as analysed in Chapter 2, the rise of an increasing relevant dimension of European constitutional law has mitigated the goals of the internal market and the predominance of self-regulation. The European orientation to dignity explains why the rise of private powers is seen as a threat to fundamental rights and democratic values. Unlike the US, the Union's dimension oriented to welfare goals does not allow capitalistic logics to prevail over the social dimension of the European market. This could provide clues about the failure of the European model to promote the creation of businesses able to compete with US tech giants. At the same time, the need to ensure competition in the internal market blocks the

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

[58] Genia Kostka, 'China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval' (2019) 21(7) New Media & Society 1565; Fan Liang and others, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure' (2018) 10(4) Policy & Internet 415.

[59] Yu Hong, *Networking China: The Digital Transformation of the Chinese Economy* (University of Illinois Press 2017).

[60] Madison Cartwright, 'Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle' (2020) 9(3) Internet Policy Review https://policyreview.info/node/1494/pdf accessed 21 November 2021.

creation of large corporations while limiting the possibility for Member States' aid to their businesses. Furthermore, the democratic constitutional basis of the Union precludes any attempt to increase surveillance over the Internet while leaving the doors open to online platforms operating on a transnational scale.

Therefore, even in this case, the path of European digital constitutionalism suggests a third way at the intersection between public authority and private ordering. The Union has not shown either its intention to leave the market free to determine the values of the algorithmic society or the interest in intervening in the market to support internal businesses in the rush for becoming a standard-maker in the algorithmic society. Even if the Artificial Intelligence Act provides a top-down approach where the Commission is at the forefront in defining the degree of risk, thus without apparently leaving spaces for self-regulation or collaboration, it is possible to consider how the Digital Services Act Package and the GDPR show how the Union is struggling to find a proportionate balance between hard and self-regulation. The Digital Services Act is not just a new legal framework to strengthen the internal market and foster the development of digital services, thus promoting innovation.[61] As in the case of the GDPR, it could be considered another way to rise as a global model for regulating transnational powers while protecting democratic values. The two pillars of this package consist of proposing clear rules for framing digital services responsibilities and ex ante rules applying to large online platforms acting as gatekeepers, which now set the rules of the game for their users and their competitors.[62]

Likewise, the GDPR can be considered a hybrid solution between regulation and self-regulation. As stressed in Chapter 6, the GDPR is a peculiar legal instrument. The risk-based approach leaves margins of discretion for public and private actors when implementing their data processing. In a certain sense, the Union's approach can be considered as an attempt to regulate digital capitalism at the intersection between market logics and democratic values. Put another way, it constitutes

[61] COM(2020) 37 final (n. 2).

[62] See Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services European Commission, Inception impact assessment – Ares(2020)2877686; Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market Inception impact assessment – Ares(2020)2877647.

a hybrid approach defining that value framework of principles and rules whose boundaries are left to the implementation of transnational businesses under the oversight of judicial power and independent competent authorities.

The European approach increasingly tends to promote a governance approach where online platforms are considered regulated centres of collaboration or digital utilities. As underlined in Chapter 3, the ability of these actors to govern content and data is not only a risk but also an opportunity to enforce public policies online. The pandemic has fostered this trend where online platforms have shown their predominant role. This situation has underlined the relevance of digital technologies for remote activities and delivery services.[63] For instance, without controlling moderation of content, disinformation and hate speech would spread online. Besides, in the field of data, the example of contact tracing apps is paradigmatic of how Google and Apple have been able to provide a global tracking application, thus capturing the attention of governments.[64]

Some platforms perform a role beyond the mere provision of services. While it may be argued that they have an editorial role which should be shielded by the protection of the right to free speech,[65] other scholars underline their role as information or privacy fiduciaries,[66] or as public utilities like infrastructures.[67] The primary challenge is not to oppose

[63] Daisuke Wakabayashi and others, 'Big Tech Could Emerge from Coronavirus Crisis Stronger Than Ever' The New York Times (23 March 2020) www.nytimes.com/2020/03/23/technology/coronavirus-facebook-amazon-youtube.html accessed 21 November 2021.

[64] Oreste Pollicino, 'Contact tracing and COVID-19: Commission and Member States agree on specifications' EU Law Live (16 June 2020) https://eulawlive.com/contact-tracing-and-covid-19-commission-and-member-states-agree-on-specifications/ accessed 21 November 2021.

[65] Eric Goldman, 'Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)' Knight First Amendment Institute (February 2018) https://knightcolumbia.org/content/course-first-amendment-protects-google-and-facebook-and-its-not-close-question accessed 21 November 2021.

[66] Jack M. Balkin, 'The Fiduciary Model of Privacy' (2020) 134(1) Harvard Law Review Forum 11; Jack M. Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis Law Review 1183.

[67] Jean-Christophe Plantin and others, 'Infrastructure studies meet platform studies in the age of Google and Facebook' (2018) 20(1) New Media & Society 293; K. Sabeel Rahman, 'Monopoly Men' Boston Review (11 October 2017) http://bostonreview.net/science-nature/k-sabeel-rahman-monopoly-men accessed 21 November 2021; Cale Guthrie Weissman, 'Maybe It's Time to Treat Facebook Like a Public Utility' Fast Company (1 May 2017) www.fastcompany.com/40414024/maybe-its-time-to-treat-facebook-like-a-public-utility accessed 21 November 2021; Danah Boyd, 'Facebook Is a Utility; Utilities Get Regulated' Apophenia (15 May 2010) www.zephoria.org/thoughts/archives/

their bigness but rather to regulate their power coming from a governance of social infrastructure. As underlined by Rahman, 'where private actors accumulate outsized control over those goods and services that form the vital foundation or backbone of our political economy – social infrastructure – this control poses dangers'.[68] The Council of Europe highlighted the increasing privatisation of public functions, particularly observing that '[w]hen such systems are then withdrawn for commercial reasons, the result can range from a decrease in quality and/or efficiency to the loss of services that are considered essential by individuals and communities'. In these cases, '[s]tates should put contingencies in place to ensure that essential services remain available irrespective of their commercial viability, particularly in circumstances where private sector actors dominate the market in ways that place them in positions of influence or even control'.[69]

Within this framework, the concept of public utilities could lead to a solution to find a balanced approach between public authority and private ordering. The increasing control over large parts of political, economic and social life leads online platforms to be critical and essential infrastructures.[70] This consolidation of power is relevant not only for individuals but also for the market. The services provided by Google or Facebook play an important role in the success of online content providers like traditional media outlets or influencers. The dominance of these actors is not limited to consumer retail sales but also the power over other business sectors relying on their services. It is not by coincidence that the Union has adopted a legal instrument to increase fairness and transparency for business users of online intermediation services.[71]

However, there is much more beyond economic power. The power of platforms to influence policy-makers and users' behaviours is a dangerous trend for constitutional democracies. In the US framework, Crawford underlines common carriage concerns would lead to overcoming First Amendment protection without requiring undue speech

2010/05/15/facebook-is-a-utility-utilities-get-regulated.html accessed 21 November 2021.

[68] K. Sabeel Rahman, 'The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept' (2018) 39 Cardozo Law Review 1621, 1625.

[69] CM/Rec(2020)1 (n. 30).

[70] Nikolas Guggenberger, 'Essential Platforms' (2021) 24 Stanford Technology Law Review 237.

[71] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (2019) OJ L 186/57.

restraints.[72] Similarly, in the field of search engines, Pasquale underlined the threats beyond individual privacy including a range of biased and discriminatory information results.[73] A framework of public utilities would lead online platforms to perform their business while increasing oversight and fairness. Facebook could be encouraged to ensure more diversity in the organisation of content while Amazon could be required to treat all retailers equally. The idea is not to oppose these social infrastructures which are increasingly critical in daily lives but to preclude their social power from overcoming the protection of constitutional values underpinning a democratic society. From services in the market, online platforms have increasingly acquired a foundational or infrastructural role in the algorithmic society. Therefore, the power of online platforms coming from the governance of digital infrastructures would deserve a regulatory framework to protect democratic values in the long run.

This new approach to digital utilities would not push constitutional democracies back to the end of the last century and lead to following a neoliberal perspective based on unaccountable cooperation between the public and private sector. Unlike at the advent of the Internet, the Union can rely on a precedent showing the challenges of going back to digital liberalism at the dawn of artificial intelligence technologies. The new phase of European digital constitutionalism shows that the Union is aware of this situation. Therefore, the primary challenge for the Union in the algorithmic society is how to ensure that the values underpinning these technologies are not entirely determined by unaccountable powers but shaped by democratic processes based on transparent and accountable procedures. This would not mean intervening in the market but providing a common regulatory frame of values and principles based on which private actors may perform their businesses. The overarching value of human dignity can limit the consolidation of powers which abuse constitutional rights.

To ensure that European values at the intersection between digital humanism and capitalism are not left to the determination of private actors, the Union is relying on a mix of hard and co-regulatory strategies. As underlined by Marsden, co-regulation entails that 'the regulatory regime is made up of a complex interaction of general legislation

[72] Susan Crawford, 'First Amendment Common Sense' (2014) 127 Harvard Law Review 2343.

[73] Frank Pasquale, 'Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines' (2008) University of Chicago Legal Forum 263.

and a self-regulatory body'.[74] Put another way, the European governance strategy is oriented towards avoiding the autonomous constitutionalisation of self-regulation.[75] As clarified in the white paper on artificial intelligence, '[i]t is also essential to make sure that the private sector is fully involved in setting the research and innovation agenda and provides the necessary level of co-investment. This requires setting up a broad-based public private partnership, and securing the commitment of the top management of companies'.[76] The Council of Europe has stressed that states should establish appropriate levels of transparency with regard to the public procurement, use, design and basic processing criteria and methods of algorithmic systems implemented by and for them, or by private sector actors. Even more importantly, it underlined that 'the legislative framework for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose'.[77] To face the adverse human rights impacts of artificial intelligence, it is worth working on 'ethics labels or seals for algorithmic systems to enable users to navigate between systems',[78] while ensuring 'particularly high standards as regards the explainability of processes and outputs'.[79]

Co-regulation implemented through different systems like public-private partnerships or public utilities regulation would be the third way that digital constitutionalism would be promoted in the European framework. Between granting a a hard regulation of the digital environment and leaving the private sector to establish the predominant values, the Union is defining a constitutional framework in between where it provides the values guiding private actors. This form of co-regulation would lead online platforms not to exercise discretionary powers on fundamental rights and democratic values, but as regulated entities driven by a mix of profit maximisation and public purposes. The focus of the Council of Europe, and also the ad-hoc committee on artificial intelligence, known as CAHAI,[80] on the introduction of algorithmic

[74] Christopher Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011).
[75] Julia Black, 'Constitutionalising Self-Regulation' (1996) 59 Modern Law Review 24.
[76] COM(2020) 65 final (n. 9).
[77] CM/Rec(2020)1 (n. 30).
[78] Ibid.
[79] Ibid.
[80] CAHAI, 'Feasibility Study on a Legal Framework on AI Design, Development and Application based on Council of Europe's Standards' (17 December 2020)

impact assessment is an evident example of the European way to increase the accountability of the public and private sector when implementing artificial intelligence technologies.[81] As observed by the Council of Europe, '[p]rivate sector actors engaged in the design, development, sale, deployment, implementation and servicing of algorithmic systems, whether in the public or private sphere, must exercise due diligence in respect of human rights'.[82]

Considering the global reach and dissemination of algorithmic technologies, this framework would increasingly underline the role of the Union as a global regulator. Put another way, rather than governing or neglecting market dynamics, the Union is tailoring its role between public authority and private ordering. Nonetheless, being a global regulator would clash with traditional territorial limits to the exercise of sovereign powers. Even if the Union is proposing its approach to algorithmic technologies on a global scale, still the hybrid approach between hard and self-regulation meets constitutional limits. Therefore, the next subsection addresses the third trade-off focusing on whether digital constitutionalism increases the tendency towards extraterritoriality of European values or, instead, promotes a phase of constitutional protectionism to avoid external interferences undermining fundamental rights and democratic values.

7.4 Scope: Constitutional Imperialism versus Constitutional Protectionism

The transnational dimension characterising the values and governance of the algorithmic society leads to focusing on how far European digital constitutionalism could extend its influence to protect fundamental rights and democratic values. If, on the one hand, the Union has proven to be oriented towards a sustainable development of algorithmic technologies and adopting a hybrid governance strategy between public values and private ordering, being a global regulator entails dealing with the external limits of sovereign powers. Territory is the natural limitation of state

www.coe.int/en/web/artificial-intelligence/-/the-feasibility-study-on-ai-legal-standards-adopted-by-cahai accessed 21 November 2021.

[81] Ibid.

[82] Ibid.

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

sovereignity. Inside that space, citizens are expected to comply with the applicable law in that area while, outside this framework, they would be subject to the influence of other sovereign powers.

As stressed in Chapter 3, the Internet, as an expression of globalisation, has challenged the traditional model to exercise sovereign powers. At the same time, the global reach of digital technologies does not necessarily leave states unarmed against overseas interferences. The cases of China and Russia show how these countries propose alternatives for governing digital technologies which tend to reflect their values.[83] Such influence has not only been domestic but also international. Together with the approach of Russia,[84] China has already tried to dismantle the western multi-stakeholder model by proposing to move Internet governance within the framework of the International Telecommunications Union in 2012.[85]

In the fight for digital sovereignty,[86] countries are following different strategies also in relation to platform power. On the one hand, still the First Amendment provides a shield against any public interference leading US companies to extend their powers and standards of protection beyond its territory. Despite some attempts to deal with platform power at the federal level,[87] and even at the local,[88]

[83] Dennis Broeders and others, 'Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' The Hague Program for Cyber Norms Policy Brief (November 2019) www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace accessed 21 November 2021; Stanislav Budnitsky and Lianrui Jia, 'Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance' (2018) 21(5) European Journal of Cultural Studies 594.

[84] Eva Claessen, 'Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU' (2020) 5(1) Journal of Cyber Policy 140.

[85] Julia Bader, 'To Sign or Not to Sign. Hegemony, Global Internet Governance, and the International Telecommunication Regulations' (2019) 15(2) Foreign Policy Analysis 244.

[86] Julia Pohle, 'Digital Sovereignty' (2020) 9(4) Internet Policy Review https://policyreview.info/pdf/policyreview-2020-4-1532.pdf accessed 21 November 2021. Stephane Couture and Sophie Toupin. 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' (2019) 21(10) New Media & Society 2305. See also Milton L. Mueller, 'Against Sovereignty in Cyberspace' (2020) 22(4) International Studies Review 779; Benjamin H. Bratton, *The Stack. On Software and Sovereignty* (MIT University Press 2016).

[87] See, e.g., the Platform Accountability and Consumer Transparency (PACT) Act (2020).

[88] See, e.g., Sofia Andrade, 'Florida's New Pro-Disney, Anti-Facebook and Twitter Law' Slate (25 May 2021) https://slate.com/technology/2021/05/florida-stop-social-media-censorship-act-disney.html accessed 21 November 2021.

nonetheless, such a liberal approach does not only foster private ordering but also hides an indirect and omissive way to extend constitutional values beyond territorial boundaries. Rather than intervening in the market, the US has not changed its role while observing its rise as a liberal hub of global tech giants. As stressed in Chapter 3, regulating online platforms in the US could affect the smooth development of the leading tech companies in the world while also increasing the transparency of the cooperation between the governments and online platforms in certain sector like security, thus unveiling the invisible handshake.[89] Snowden's revelations have already underlined how far public authorities rely on Internet companies to extend their surveillance programme and escape accountability.[90] Put another way, the US digital sovereignty would benefit from private ordering and the invisible cooperation between public and private actors.

On the other hand, China has always controlled its market from external interferences rather than adopting a liberal approach or exporting values through international economic law. China is only imitating the western conception of the Internet while maintaining control over its businesses. Baidu, Alibaba and Tencent, also known as BAT, are increasingly competing with the dominant power of Google, Apple, Facebook, Amazon, or GAFA. The international success of TikTok is an example of how China aims to attract a global audience of users while supporting its business sector.[91] Besides, the adoption of the Digital Silk Road increasingly makes China a relevant player beyond territorial boundaries. The Huawei model is based on exporting technological power supplying digital infrastructure even in peripheral areas. Put another way, China is only partially opening to digital globalisation while it is maintaining control over the network architecture. This twofold approach is part of what has been called the Beijing effect.[92]

[89] 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.

[90] David Lyon, *Surveillance after Snowden* (Polity Press 2015).

[91] Michael Keane and Haiqing Yu, 'A Digital Empire in the Making: China's Outbound Digital Platforms' (2019) 13 International Journal of Communication 4624.

[92] Matthew S. Erie and Thomas Streinz, 'The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance' SSRN (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256 accessed 21 November 2021.

The Union has already shown its ability to influence global dynamics, so that scholars have named such an attitude the 'Brussels effect'.[93] The Union is increasingly aware of its ability to extend its 'regulatory soft power', influencing the policy of other areas of the world in the field of digital technologies. It should not surprise that the Union has also started to build its narrative about digital sovereignty.[94] As underlined by the Commission, 'European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks and communications' aimed to mitigate 'dependency on other parts of the globe for the most crucial technologies'.[95] This approach does not entail closing European boundaries towards a form of constitutional protectionism but to ensure Europe's ability to define its rules and values in the digital age. Indeed, 'European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model',[96] and, as a result, 'the EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based'.[97] These statements suggest that the Union is taking its path towards a leading role in regulating the digital environment and artificial intelligence technologies. Rather than focusing just on promoting the European industry, the Union approach is oriented towards rising as a global standard-maker. Its narrative is not adversarial but cooperative towards external actors while, at the internal level, it is not possible to foresee how digital sovereignty will be articulated at the supranational level or driven by Member States' single actions. This is also why the fight for digital sovereignty is particularly relevant on the external and internal level, especially for the Union.[98]

The GDPR shows the intention of the Union to act as a global regulator. The long arm of European data protection law has been already highlighted in the framework of the Data Protection Directive,[99]

[93] Anu Bradford, *The Brussels Effect. How the European Union Rules the World* (Oxford University Press 2020). See also Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2018) 62 American Journal of Comparative Law 87.

[94] COM(2020) 67 final (n. 7), 2.

[95] Ibid., 2.

[96] Ibid.

[97] Ibid.

[98] Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 Philosophy and Technology 369.

[99] Lokke Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1(1) International Data Privacy Law 28.

defining the 'global reach of EU law'.[100] The European framework of data protection is finding its path on a global scale,[101] while raising as a model for other legislations across the world.[102] The UN secretary-general has welcomed the European approach by underlining how this measure is inspiring for other countries and encouraged the Union and its Member States to follow this path.[103] Furthermore, the adoption of the GDPR has led a growing number of companies to voluntarily comply with some of the rights and safeguards even for data subjects outside the territory of the Union because protecting privacy and personal data has become a matter of reputation.[104] The recent spread of the pandemic has shown the relevance of data protection safeguards for constitutional democracies when dealing with contact tracing applications or other forms of public surveillance.[105]

Besides, the GDPR has not only become a model at the global level but also provides a scope of application which would extend beyond the European territory. Precisely, even though the data controller is established outside the Union, European data protection law is nevertheless applicable if the processing of personal data implies the provision of products or services to data subjects who are in the Union, and the processing activities are related either to the offering of goods and services in the EU, or to the monitoring of the behaviour of data subjects in the EU.[106] By extending the scope of application of the GDPR also outside the EU framework, the Union adopts a form of constitutional imperialism by imposing its own legal standard of protection on a global scale.

[100] Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019).

[101] Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYU Law Review 771.

[102] Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 Privacy Laws & Business International Report 14.

[103] Address of the UN Secretary-General to the Italian Senate, 18 December 2019 www.un.org/press/en/2019/sgsm19916.doc.htm accessed 21 November 2021.

[104] Cisco, 'Consumer Privacy Study. The Growing Imperative of Getting Data Privacy Right (November 2019) www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf accessed 21 November 2021.

[105] Oreste Pollicino, 'Fighting COVID-19 and Protecting Privacy under EU Law. A Proposal Looking at the Roots of European Constitutionalism' EU Law Live (16 May 2020) https://eulawlive.com/weekend-edition/weekend-edition-no17/ accessed 21 November 2021.

[106] GDPR (n. 17), Art. 3(2).

Nonetheless, while it is true that the GDPR is rising as a global model for the protection of privacy and personal data, it is not driven by a mere goal of extraterritoriality or imperialism. Rather, it shows that the Union aims to ensure that formal territorial limitations do not undermine the protection of fundamental rights of privacy and data protection and the related democratic values in the Union. The extraterritorial reach of European data protection law and, in general, of the GDPR can be considered as an 'anti-circumvention mechanism'.[107] The ECJ has contributed to explaining the need to extend European rules to ensure the effective protection of fundamental rights. The GDPR territorial scope of application has codified the doctrine of establishment developed by the ECJ in *Weltimmo* and *Google Spain*.[108] In *Weltimmo*, the ECJ adopted a broad interpretation of the concept of 'establishment' avoiding any formalistic approach linked to the place registration of companies. Likewise, in *Google Spain*, the ECJ underlined this flexible interpretation '[i]n the light of the objective pursued by Directive 95/46, consisting in ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data'.[109] The consequence of such a rule is twofold. On the one hand, this provision involves jurisdiction. The GDPR's territorial scope of application overcomes the doctrine of establishment developed by the ECJ's case law, since even those entities that are not established in the EU will be subject to the GDPR. On the other hand, the primary consequence of such an extension of territoriality is that of extending European constitutional values globally.

The intention to overcome territorial formalities also drove the ECJ in the *Schrems* case,[110] when it invalidated the Commission's adequacy decision,[111] known as the 'safe harbour agreement', concerning the transfer of personal data from the EU to the United States. In this case, it is possible to observe another manipulation of data protection law

[107] Svetlana Yakovleva and Kristina Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation' (2020) 114 AJIL Unbound 10.

[108] C-230/14 *Weltimmo s.r.o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság* (2015).

[109] C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014).

[110] Case C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner* (2015).

[111] 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.

extending its boundaries across the Atlantic. Although the Data Protection Directive required US data protection law to ensure an 'adequate' level of protection,[112] the ECJ went beyond this boundary by stating that the safeguards should be 'equivalent' to those granted by EU law to ensure the effective protection of the fundamental rights to privacy and data protection as enshrined in the Charter.[113]

However, this decision did not exhaust the concerns about the safeguards in the transfer of personal data across the Atlantic. The ECJ invalidated the new adequacy decisions (i.e. Privacy Shield),[114] in light of the protection of fundamental rights as also translated into the new framework for personal data transfer introduced by the GDPR.[115] The ECJ went even further assessing the Standard Contractual Clauses (SCCs) framework. Even without invalidating the Commission Decision on the use of these clauses,[116] the ECJ underlined that the equivalent level of protection applies even to this legal instrument. The court expressly underlined the limits of EU law in relation to third countries since SSCs are not capable of binding the authorities of that third country.[117] Therefore, the ECJ recognised the role of the controller established in the Union and the recipient of personal data to check and monitor whether the third country involved ensures an essentially equivalent degree of protection.[118] When this is not the case, the ECJ does not preclude the transfer but underlines the need to set additional safeguards to ensure that degree of protection.[119]

This system has recognised the freedom of business actors to define the standard of protection of personal data across the Atlantic. Besides,

[112] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31, Art. 25.

[113] Oreste Pollicino and Marco Bassini, 'Bridge Is Down, Data Truck Can't Get Through . . . A Critical View of the Schrems Judgment in the Context of European Constitutionalism' (2017) 16 The Global Community Yearbook of International Law and Jurisprudence 245.

[114] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016) OJ L 207/1.

[115] C-311/18 *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximillian Schrems* (2020).

[116] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010) OJ L 39/5.

[117] Ibid., 136.

[118] Ibid., 135, 137, 142.

[119] Ibid., 133.

Daskal underlined the limits of the entire system since 'there is no guarantee that the companies will win such challenges; they are, after all, ultimately bound by U.S. legal obligations to disclose. And even more importantly, there is absolutely nothing that companies can do to provide the kind of back-end judicial review that the Court demands'.[120]

While these questions are still open, it cannot be excluded that this over-reaching scope of protection beyond European boundaries could affect free speech and the financial interests of other countries and their citizens,[121] and decrease the degree of legal certainty leading to a binary approach which is not scalable.[122] The GDPR has also been criticised for its 'privacy universalism'.[123] Proposing the GDPR as a global model entails exporting a western conception of privacy and data protection that could clash with the values of other areas of the world, especially in peripheral areas of the world, thus opening a new phase of (digital) colonialism together with the US and China.[124]Although other scholars do not share the same concerns, they have observed that 'when a law is applicable extraterritorially, the individual risks being caught in a network of different, sometimes conflicting legal rules requiring simultaneous adherence. The result – conflicts of jurisdiction – may put an excessive burden on the individual, confuse him or her, and undermine the individual's respect for judicial proceedings and create loss of confidence in the validity of law'.[125]

The ECJ has recently highlighted these challenges in the decision *Google* v. *CNIL* where the core of the preliminary questions raised by the French judge aimed to clarify the boundaries of the right to be

[120] Jennifer C. Daskal, 'What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers' Just Security (17 July 2020) www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/ accessed 21 November 2021.

[121] Dan J. B. Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3(4) International Data Privacy Law 278, 1.

[122] Christoper Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235.

[123] Payal Arora, 'GDPR – A Global Standard? Privacy Futures, Digital Activism and Surveillance Cultures in the Global South' (2019) 17(5) Surveillance & Society 717.

[124] Micheal Kwet, 'Digital Colonialism: US Empire and the New Imperialism in the Global South' (2019) 60(4) Race & Class 3; Danielle Coleman, 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) 24 Michigan Journal of Race & Law 417.

[125] Paul De Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6(3) International Data Privacy Law 230, 240.

forgotten online, especially its global scope.[126] Within this framework, the ECJ ruled on a preliminary reference concerning the territorial scope of the right to be forgotten online.

The court observed that the scope of the Data Protection Directive and the GDPR is to guarantee a high level of protection of personal data within the Union and, therefore, a de-referencing covering all the domains of a search engine (i.e. global delisting) would meet this objective. This is because the role of search engines in disseminating information is relevant on a global scale since users can access links to information 'regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself'.[127]

Nevertheless, the ECJ underlined the limits of this global approach. Firstly, states around the world do not recognise the right to delist or provide different rules concerning the right to be forgotten online.[128] Even more importantly, since the right to privacy and data protection are not absolute rights, they need to be balanced with other fundamental rights,[129] among which the right to freedom of expression.[130] The protection of these fundamental rights (and, therefore, their balance) is not homogenous around the world. The GDPR does not aim to strike a fair balance between fundamental rights outside the territory of the Union.[131] Before this crossroads, rather than extending the boundaries of data protection law to the global scale, the ECJ followed the opinion of Advocate General Szpunar,[132] thus observing that neither the Data Protection Directive nor the GDPR recognises the right of data subjects to require a search engine like Google to delist content worldwide.[133]

Therefore, although Google falls under the scope of European data protection law, it is not required to delist information outside the territory of Member States. Nonetheless, Member States still maintain the possibility to issue global delisting orders according to their legal framework. The ECJ specified that if, on the one hand, EU law does not require search

[126] Case C-507/17, *Google Inc.* v. *Commission nationale de l'informatique et des libertés (CNIL)* (2019).
[127] Ibid., 57.
[128] Ibid., 58.
[129] Ibid., 59.
[130] See Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* v. *Land Hessen* (2010) ECR I-11063, 48; Opinion 1/15 EU-Canada PNR Agreement (2017), 136.
[131] GDPR (n. 17) Art. 17(3)(a).
[132] Opinion of Advocate General in C-507/17 (n. 126), 63.
[133] C-507/17 (n. 126), 64.

engines to remove links and information globally, on the other hand, it does not ban this practice. It is for Member States to decide whether extending the territorial scope of judicial and administrative order according to their constitutional framework of protection of privacy and personal data balances with the right to freedom of expression.[134]

The ECJ also explained that the impossibility to require search engines to delist information on a global scale is the result of the lack of cooperation instruments and mechanisms in the field of data protection. The GDPR only provides the supervisory authorities of the Member States with internal instruments of cooperation to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data against the interest of the public in various Member States in having access to information.[135] Therefore, such instruments of cooperation cannot be applied outside the territory of the Union.

Regarding the second question, concerning the territorial scope of delisting within the territory of the Union, the ECJ observed that the adoption of the GDPR aims to ensure a consistent and high level of protection of personal data in all the territory of the Union and, therefore, delisting should be carried out in respect of the domain names of all Member States.[136] Nonetheless, the ECJ acknowledged that, even within the Union, the interest to accessing information could change between Member States as also shown by the degree of freedom Member States enjoy in defining the boundaries of processing in the field of freedom of expression and information pursuant to Article 85 of the GDPR.[137] In other words, the ECJ underlined not only that freedom of expression does not enjoy the same degree of protection at the international level but also, in Europe, it can vary from one Member State to another. Therefore, it is not possible to provide a general obligation to delist links and information applying to all Member States.

To answer this issue, the court left this decision to national supervisory authorities which through the system of cooperation established by the GDPR should, inter alia, reach 'a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all

[134] Case C-617/10, *Åklagaren* v. *Hans Åkerberg Fransson* (2013), 29; C-399/11, *Stefano Melloni* v. *Ministerio Fiscal* (2013), 60.
[135] GDPR (n. 17), Arts. 56, 60–6.
[136] C-507/17 (n. 126), 66.
[137] Ibid., 67.

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

its establishments in the Union'.[138] Likewise, also with respect to geo-blocking techniques, the ECJ did not interfere with Member States' assessment about these measures but simply recalled, by analogy, that 'these measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging Internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name'.[139] By distancing itself from Advocate General Szpunar's view on this point,[140] the ECJ decided not to recognise a general removal obligation at the European level but relied on the mechanism of cooperation of national authorities as well as on the discretion of Member States concerning preventive measures.

Just one week later, in *Glawischnig-Piesczek* v. *Facebook*,[141] the court addressed the territorial extension of national injunctions concerning the removal of content. The ECJ observed that the e-Commerce Directive does not provide for any limitation to the territorial scope of the measures that Member States can adopt and, consequently, EU law does not prevent a national order from extending its scope application globally. As a general limit, the ECJ specified that Member States should take into consideration their international obligations given the global dimension of the circulation of content, without either specifying which rules of international law would apply in this case.

With regard to the territorial extension of national orders, the ECJ did not clarify to which rules of international law the Member States should refer to assess the territorial scope of removal orders. Some perspectives on this point can be found in the decision *Google* v. *CNIL*. In this case, the ECJ expressly refers to the potential contrast of a global delisting order with the protection of rights at an international level. Therefore, national competent authorities can strike a fair balance between individuals' right to privacy and data protection with the right to freedom of information. However, the different protection of freedom of expression at a global level would limit the application of the balancing results. Advocate General Szpunar reaches the same conclusion in the Facebook case, explaining that, although EU law leaves Member States

[138] Ibid., 68.
[139] Ibid., 70. See, inter alia, Case C-484/14, *Tobias McFadden* v. *Sony Music Entertainment Germany GmbH* (2016), 96.
[140] Opinion of Advocate General in C-507/17 (n. 126), 78.
[141] Case C-18/18, *Eva Glawischnig-Piesczek* v. *Facebook* (2019).

free to extend the territorial scope of their injunctions outside the territory of the Union, national courts should limit their powers to comply with the principle of international comity.[142]

This trend towards local removal is based not only on the status quo of EU law at the time of the decisions but also on the effects that a general extension of global remove can produce in the field of content and data. As observed by Advocate General Szpunar, a worldwide de-referencing obligation could initiate a 'race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale'.[143] In other words, the ECJ's legitimacy could start a process of cross-fertilisation, thus leading other countries to extend their removal order on a global scale. This could be particularly problematic when looking at authoritarian or illiberal regimes which could exploit this decision to extend their orders, or, more generally, the scope of their system beyond their territories.

Moreover, in *Google* v. *CNIL*, the ECJ explained that the limit for global removal also comes from the lack of intention to confer an extraterritorial scope to the right to erasure established by the GDPR.[144] The lack of cooperation mechanisms between competent authorities extending outside the territory of the Union would confirm this argument. Nevertheless, by supporting this position, the ECJ did not consider that, more generally, the GDPR establishes a broad territorial scope of application covering processing activities related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.[145]

Nonetheless, it is worth underlining that the Union has not closed the doors to the possibility of extending the territorial scope of removal orders beyond EU borders. At first glance, the ECJ seems to express an opposite view in the two cases regarding the territorial scope of national orders. On the one hand, in *Google* v. *CNIL*, the ECJ stated that EU law does not require search engines to carry out the delisting of information and links on a global scale. In *Glawischnig-Piesczek* v. *Facebook*, on the other hand, the ECJ explained that there are no obstacles to global removal, but also leaves the evaluation to Member States.

[142] Opinion of Advocate General in C-18/18 (n. 141), 100.
[143] Ibid., 61.
[144] C-507/17 (n. 126), 62.
[145] GDPR (n. 17), Art. 3(2).

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

Although the two judgments may seem opposite, they lead to the same result, namely that EU law does not either impose nor preclude national measures whose scope extends worldwide. This is a decision which rests with Member States which are competent to assess their compliance with international obligations. The e-Commerce Directive does not provide a specific territorial scope of application and the ECJ has not gone further. Otherwise, 'it would have trespassed within the competencies of Member States, which under EU law retain primary legislative power on criminal law matters'.[146] Besides, the reasons for this different approach can be attributed to the different degree of harmonisation of the protection of personal data and defamation as observed by Attorney General Szpunar.[147] Therefore, it is not just an issue concerning public international law but also private international law contributes to influencing the territorial scope of removal orders.[148]

Despite the relevance of this point, leaving Member States free to determine when a national order should be applied globally could lead to different national approaches which would fragment harmonisation goals. This situation is particularly relevant in the framework of the GDPR since it provides a new common framework for Member States in the field of data. While the content framework still relies on the e-Commerce Directive, leaving margins of discretion to Member States, this approach in the field of data is more problematic. On the one hand, the GDPR extends its scope of application to ensure a high degree of protection of fundamental rights of the data subjects. On the other hand, such a framework can be questioned by the autonomy of Member States to decide the reach of the right to be forgotten online. As Zalnieriute explains, '[b]y creating the potential for national data protection authorities to apply stronger protections than those afforded by the GDPR, this decision could be seen as another brick in the "data privacy wall" which the ECJ has built to protect EU citizens'.[149]

[146] Elda Brogi and Marta Maroni, 'Eva Glawischnig-Piesczek v Facebook Ireland Limited: A New Layer of Neutrality' CMPF (7 October 2010) https://cmpf.eui.eu/eva-glawischnig-piesczek-v-facebook-ireland-limited-a-new-layer-of-neutrality/ accessed 21 November 2021.

[147] Opinion Advocate General in C-18/18 (n. 141), 79.

[148] Paolo Cavaliere, 'Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations' (2019) 4 European Data Protection Law 573, 577.

[149] Monika Zalnieriute, 'Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)' (2020) 114(2) American Journal of International Law 261.

Furthermore, even in this case, the ECJ has not focused on the peculiarities of platform activities and the consequences of these decisions on the governance of freedom of expression in the digital space. In *Glawischnig-Piesczek* v. *Facebook*, a local removal order would not eliminate the possibility of accessing the same content – identical or equivalent – through the use of other technological systems or outside the geographical boundaries envisaged by the removal order. This problem is particularly relevant in *Google* v. *CNIL* since it is possible to access different Google domain names around the world easily. The interest in the protection of reputation could also require an extension beyond the borders of the Union to avoid relying just on partial or ineffective remedies. The ECJ recognised that access to the referencing of a link referring to information regarding a person in the Union is likely to have 'immediate and substantial effects on the person'.[150] Therefore, even if this statement is just one side of the balancing activity with the protection of international law on the other side, it leads to contradictory results frustrating data subjects' right to be forgotten due to the potential access to search engines' domain names. Furthermore, to comply with geographical limits, geo-blocking and other technical measures would require an additional effort for platforms, thus increasing the risk of censorship on a global scale and creating a technological barrier for small-medium platforms.

It is possible to observe how one of the consequences of this approach is to increase the regulatory burdens for those entities which, although not established in the Union territory, offer goods and services or monitor the behaviour of data subjects in the Union. In other words, the Union is trying to ensure that formal geography could not constitute a shield to avoid compliance with any regulation. Rather than a European constitutional imperialism, this approach would aim to protect individual fundamental rights,[151] while avoiding businesses escaping from complying with EU law just by virtue of a formal criterion of establishment. Otherwise, the primary risk is to encourage a disproportionate imbalance between businesses operating physically in the territory of a state, and other entities which, by processing data and offering other digital services, would avoid complying with the law of the states in which they perform their business.

[150] C-507/17 (n. 126), 57.
[151] De Hert and Czerniawski (n. 125).

Therefore, the extraterritorial effects of European data protection law does not express a form of constitutional imperialism or protectionism. The need to ensure the protection of fundamental rights in a globalised world leads the Union to exercise a global influence which, at first glance, would be the opposite of constitutional protectionism. At the same time, the Union is aware of the consequences of the extension of constitutional values on the global scale which, according to the ECJ case law, seems to appear an exceptional resort based on Member States' assessment.

The proposal for the Artificial Intelligence Act is an example of this European approach. On the one hand, the scope of the proposal would extend to 'providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country', thus providing a broader territorial coverage which aims to ensure that European standards are taken seriously on a global scale. On the other hand, this instrument can be considered an expression of constitutional protectionism. The top-down approach of the Union, which aims to leave small margins to self-regulation, would be an attempt to protect the internal market from technological standards which would not comply with the European standard of protection, whose beacon, even if less evidently in this case, is the protection of European values and, therefore, fundamental rights and democracy. Rather than making operators accountable for developing and implementing artificial intelligence systems, the regulation aims to prevent the consolidation of standards which, even if far from European constitutional values, could however find a place in the internal market.

This way, the Union is rising as global regulator proposing a transnational model to limit interferences coming from oppressive models of governance based on a wide liberal approach or oppressive public control. In other words, rather than adopting an extraterritorial or protectionist approach, the Union seems to have chosen a third way once again. As in the case of values and governance, the Union has shown its intent to take a third way proposing its role as a global regulator rather than a liberal or authoritarian hub for tech giants. The European constitutional standard would not only promote the sustainable development of artificial intelligence in the long term but also, in the short term, limit and mitigate the competitive advantage of other States.

Such a third way is the result of the role of European digital constitutionalism which, in these years, has demonstrated how rights and

freedoms cannot be frustrated just by formal doctrines based on territory and establishment. At the same time, European digital constitutionalism does not express imperialist or protectionist goals but rather proposes a different political and normative model to protect fundamental rights and democratic values on a global scale.

7.5 Conclusions: The Constitutional Lesson Learnt and the Digital Road Ahead

The rise of European digital constitutionalism has shown to what extent the consolidation of the algorithmic society has affected constitutional values underpinning the social contract. The evolution of digital technologies has provided invaluable opportunities for the exercise of fundamental rights and democratic values while unveiling the opaque side of a new system of values and governance which aims at imposing itself globally, notwithstanding the fact that constitutional values are still rooted and fragmented in local traditions.

The unitary state and its laws is slowly replaced by the fragmentation of new institutions expressing their principles and values on a global scale. The traditional notion of the law, as an expression of public authority, seems to be increasingly nuanced and competing with norms (auto)produced by other subsystems. Put another way, from 'law and territory', this research has underlined how the relationship between 'norms and space' is increasingly relevant in the algorithmic society. Non-state actors, private corporations and supranational governance institutions contribute to defining their rules and codes of conduct whose global reach overlaps with the traditional expression of national sovereign power. This scenario should not come as a surprise. It is the inevitable result of globalisation leading to an intertwined scenario made of norms and values at the global level. Such a parallel production of standards and norms for the digital environment inevitably meets local constitutional values. States rely on the possibility to express sovereign powers enjoying the exclusive monopoly on the use of force. International organisations develop standards for the digital environment, while transnational private actors, precisely online platforms, privately determine the boundaries to moderate content and process data, thus rising as social infrastructures. In this process of mutual influence between global and local dynamics, constitutional values are just a small piece of the jigsaw.

https://doi.org/10.1017/9781009071215.008 Published online by Cambridge University Press

This research has demonstrated how, in this framework of legal pluralism defining interrelated normativities, the talent of European constitutionalism has provided a first reaction oriented to the protection of fundamental rights and democratic values in the algorithmic society. The answer to the first research question, 'what are the reasons for the rise of European digital constitutionalism?', has focused on underlining the path leading the Union to move from digital liberalism to a democratic constitutional approach. Vis-à-vis the constitutionalisation of global systems, the Union has entered into a new digital constitutional phase. Chapter 2 analysed how, at the end of the last century, the Union adopted a digital liberal approach oriented to trust in the ability of the internal market to grow thanks to the development of new digital products and services. The fear of overwhelming the market and slowing down the development of this promising technological framework governed the European approach at the end of the last century. The strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were going to revolutionise the entire society and promise new opportunities. The minimum harmonisation adopted in the field of content and data can be considered two examples of the neoliberal approach characterising the first phase of the Union's approach to the digital environment.

The end of this phase was the result of two events which, at the very least, have led to the end of the first (liberal) phase and trigger a new phase of the European path characterised by the role of the ECJ in paving the way towards digital constitutionalism through judicial activism. Precisely, the emergence of the Nice Charter as a bill of rights and the increasing relevance of globalised dynamics and the consolidation of private powers in the digital environment have played a critical role to move the perspective of the Union from economic freedoms to fundamental rights and democratic values. The rise of digital constitutionalism in Europe has been characterised by two primary characteristics. Firstly, the codification of the ECJ's efforts to extend the protection of fundamental rights in the digital environment has translated judicial activism into a regulatory outcome. Secondly, within the framework of the Digital Single Market strategy, the Union also clarified its intentions to limit platform powers by fostering the degree of transparency and accountability of online platforms and asking these actors to protect core values. This phase of European digital constitutionalism has shown the talent of European constitutional law in providing a first reaction

not only against public interferences but also against the exercise of digital powers by transnational private actors.

Nonetheless, the reaction of European digital constitutionalism to the challenges of the algorithmic society is not enough to explain the characteristics of digital powers. This is why the second question of this work focused on answering 'what are the characteristics and the limits to platform powers in the digital environment?'. As examined in Chapter 3, the liberal approach adopted at the end of last century has empowered online intermediaries to enforce public policies. Requiring online intermediaries to remove 'illegal' content based on their awareness is an example of delegation to the private sector of functions traditionally vested in public authorities, namely the definition of content legality. This delegation of functions has not been guided by public safeguards like due process, thus leaving online platforms to set their own procedure to moderate content and process personal data on a global scale. This way, platforms have been free to remove content or block accounts without any accountability, no matter if they affected speech on a global scale. Similar considerations can be extended to the field of data where the possibility to easily acquire or even overcome consent and the risk-based approach have recognised data controllers ample margins of discretion in defining the degree of safeguards of personal data in a certain context, thus becoming the arbiters of data protection.

Additionally, the lack of safeguards, mixed with the opportunities offered by the development of algorithmic processing technologies, has led these actors to being able to complement such delegated powers with autonomous ones. Indeed, such a new form of (digital) power is also the result of the capability to extract value from the processing of data and organisation of content through the implementation of artificial intelligence technologies. The private development of digital and automated decision-making technologies has not only challenged the protection of individual fundamental rights such as freedom of expression and data protection. This new technological framework has also empowered online platforms to perform quasi-public functions in the transnational context. It is because of this political, legal and technological framework that the freedom to conduct business has turned into power. Focusing just on the delegation of powers does not provide a clear picture of the power which online platforms exercise when discretionarily setting and enforcing rules driven by private determinations rather than constitutional values. Online platforms vertically

order the relationship with users while autonomously setting the rules to enforce and balance users' fundamental rights by using automated decision-making processes without any constitutional safeguard.

These considerations are still not enough to explain the characteristics of digital powers in the algorithmic society. Another critical piece of the constitutional puzzle is at the intersection of the legal regimes of content and data. As examined in Chapter 4, it is possible to understand the consolidation of platform powers by looking at the blurring boundaries of the legal regimes of expression and data in the algorithmic society which, in the phase of digital liberalism, have been conceived on parallel tracks. This choice, which could seem neutral at the end of the last century when online intermediaries performed passive activities, is now questioned by a digital environment made of active providers whose business model is based on the extraction of value from information.

When looking at online platforms, precisely social media and search engines, it is possible to understand the technological intersection between the legal regimes of content and data. These actors operate as data controllers when deciding the means and the purposes of processing personal data while they can also be considered processors for the data they host. On the other hand, platforms actively organise content according to the data they collect from users even if they can rely on an exemption of liability for hosting and organising third-party illicit content. The mix of content and data liability regimes makes it easier for online platforms to shield their activities in the blurring lines between the two systems. The organisation of users' content and the processing of data are part of a unique framework even if the legal regimes of content and data have been conceived on parallel tracks. In other words, the technological divergence between content and data at the end of the last century has converged towards overlapping layers of protection.

This situation leads to wondering whether European digital constitutionalism could provide a solution to the exercise of unaccountable powers in the algorithmic society. In order to unveil the normative side of this phase, the third question of this research aims to examine: 'which remedies can European constitutionalism provide to solve the imbalances of power in the algorithmic society and mitigate the risks for fundamental rights and democratic values?' The rise of digital constitutionalism has been just a first step. The talent of European constitutional law has not just led to a reaction against the rise of digital powers but also proposes a normative framework for protecting democratic values in the long run. Still, the primary issues in the field

of content and data led to thinking about the role of European constitutional law in addressing the primary challenges for fundamental rights and democracy in the algorithmic society.

As underlined in Chapter 5, protecting freedom of expression just as a liberty cannot be enough to ensure an effective protection of this fundamental right in the algorithmic society. The process of content moderation has shown how online platforms, as private actors, exercise their powers on freedom of expression on a global scale while maintaining their immunity. Despite the step forward made within the framework of the Digital Single Market strategy, users cannot rely on a clear set of transparency and accountability safeguards in the process of content moderation. They do not usually know the criteria or the logic based on which their expressions are organised and filtered or even removed. The lack of any safeguard and remedy against online platform discretion in moderating content leads to thinking about the instruments that constitutional law may provide to remedy this situation. While the horizontal application of freedom of expression could not be a general solution but just a reactive approach, rethinking media pluralism online could be another way to rely on the states' obligations to ensure not only the negative but also the positive side of freedom of expression. This shift of view would be primarily encouraged by the constitutional humus of the Union whose overarching principle of dignity would limit abuses of power annihilating the protection of other constitutional values. In this case, European constitutional law could promote a uniform regulatory framework of the procedures to moderate content. Such a normative approach would not aim to dismantle the system of platform liability nor regulate speech. Instead, as shown by the Digital Services Act, it consists of limiting platform discretion and introducing procedural safeguards in content moderation.

When moving to the field of data, the normative side of European digital constitutionalism looks slightly different. Unlike in the case of content, individuals can rely on a positive framework of safeguards which aims to mitigate private powers through instruments of transparency and accountability. The GDPR is a paradigmatic example of this approach. Nonetheless, this result does not mean that digital constitutionalism has achieved its purpose. As analysed in Chapter 6, the reactive approach of digital constitutionalism has not been enough to address the challenges of the algorithmic society to privacy and data protection. The GDPR leaves broad margins of

discretion by adopting a risk-based approach where the data controller becomes the arbiter of personal data protection. For this reason, in order to preclude such a freedom from turning into forms of power, the normative side of European digital constitutionalism in the field of data consists of providing constitutional guidance. The GDPR includes values underpinning European constitutionalism. Precisely, the principles of human dignity, proportionality and due process are the core driving values of European data protection law. These values can provide the normative interpretation on which lawmakers and courts can rely to scrutinise and mitigate data controllers' discretion, thus maintaining their accountability without overwhelming the private sector with further obligations.

The talent of European constitutionalism in reacting and proposing a normative framework to remedy the exercise of digital powers is only a starting point vis-à-vis the challenges of the algorithmic society. The fourth research question was oriented to understand: 'which paths could the consolidation of European digital constitutionalism open to the Union in the next years?' The previous sections of this chapter have underlined how digital constitutionalism could find its 'third way' to address the challenges of the algorithmic society. In front of the regulatory crossroad of the fourth industrial revolution, the Union seems to have chosen a path towards the development of a sustainable artificial intelligence environment rather than focusing simply on fostering innovation to exploit the potentialities of these technologies or merely impeding their development to protect fundamental rights and democratic values. Likewise, in order to limit autonomous determinations of public values by the private sector, the Union is rising as a global regulator whose approach is based on co-regulation. The challenges raised by self-regulation and the risk of hard regulation have led the Union to choose a third way also in this case by proposing a hybrid system of governance based on a common framework of public values guiding the determinations of the private sector. The scope of this system is another tile of the mosaic. The need to protect fundamental rights and democratic values from global challenges has not led the Union to enter into a phase of constitutional imperialism or protectionism. It has raised a balanced approach which limits the extraterritoriality of European constitutional values while narrowing the scope of formal justifications based on territorial boundaries which could substantially undermine the protection of fundamental rights and democratic values.

These challenges have led the Union to learn an important constitutional lesson. Neoliberal approaches refraining the role of public actors in protecting fundamental rights and democratic values may clash with the characteristics of European constitutionalism. Fundamental rights and democratic values cannot be left in the hands of unaccountable powers which, even if private, make decisions affecting daily lives outside democratic circuits. Against the threats coming from a ubiquitous automation which pushes the role of humans aside, European digital constitutionalism can rely on a set of safeguards and guarantees among which human dignity plays a critical role as a constitutional guidance. These characteristics would reveal the mission of European digital constitutionalism: rising as a shield against the discretionary exercise of powers which puts humans under a new *status subjectionis* driven by the logics of digital capitalism. European constitutions do not consider human beings and their identity based on capitalistic logics. European constitutionalism protects dignity even when humans do not meet the expectation of a capitalist system to protect them from its consequences, such as poverty and inequality. Within this framework, European digital constitutionalism would constitute a limit to a process of dehumanisation driven by digital capitalism. Even if the challenges of the algorithmic society cannot be compared to the horror of the last century, constitutional democracies should be concerned about the rise and consolidation of powers outside any control.

A fourth phase or a more mature expression of digital constitutionalism would aim to oppose techno-determinist solutions and contribute to promoting European values as a sustainable constitutional model for the development of automated technologies in the global context. Therefore, the primary goal of digital constitutionalism in the algorithmic society is to promote and safeguard constitutional values from the rise of unaccountable digital powers. The road ahead of digital constitutionalism is far from being straight but the path already made so far seems to be promising.