The European Union's Pursuit of Digital Sovereignty Through Legislation

by **Lukas von Ditfurth** *

Abstract: In recent years, calls for promoting Europe's digital sovereignty have gained traction in Europe, including in EU policy circles. A digitally sovereign Europe, it is hoped, will be able to more effectively and autonomously control the use of digital technologies, services, and data in Europe. This Article aims to shed light on the concept of digital sovereignty and its relevance for the EU's ongoing efforts to (re-)shape the rules of cyberspace through legislation. To this end, the Article attempts to develop a coherent understanding of digital sovereignty. Based on this understanding, the Article then analyzes how the EU has attempted to promote its digital sovereignty through legislation. It argues that the pursuit of digital sovereignty can be seen as an overarching goal and framework for a wide range of recent legal acts, including the Artificial Intelligence Act, the Digital Services Act, and the Digital Markets Act. The Article concludes by discussing the desirability of digital sovereignty as a legal and political goal and by considering some of the main criticisms of the EU's pursuit of digital sovereignty.

Keywords: Digital Sovereignty, European Union, Data Strategy, Tech Sovereignty, Technological Independence, Digital Markets, Artificial Intelligence

Recommended citation: Lukas von Ditfurth, The European Union's Pursuit of Digital Sovereignty Through Legislation, 16 (2025) JIPITEC 286 para 1.

A. Introduction

1 Digital Sovereignty has been the leitmotif of the European Commission's digital agenda during Ursula von der Leyen's first term as president. Going back to her candidacy in 2019, von der Leyen has advocated for the EU to become technologically sovereign and a global standard-setter in the digital realm.[1] Since then, the notion of digital sovereignty has featured prominently in speeches and documents from representatives and members of EU institutions.[2] At

* Dr. Lukas von Ditfurth, LL.M. (Chicago) is Associate at Hengeler Mueller Partnerschaft von Rechtsanwälten mbB, Berlin. The author is publishing this Article in his personal capacity and does not represent the views of the firm or its clients. He would like to thank the anonymous reviewer from whose thoughtful comments this Article has benefited substantially.

1 See Ursula von der Leyen, 'A Europe that strives for more: my agenda for Europe' (2019) 13 <https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf>. Even prior to von der Leyen's candidacy, the idea of European digital sovereignty had gained some traction in both scholarly and policy circles. In 2016, then Commissioner Viviane Reding stressed the crucial importance of digital sovereignty for Europe's future; see Viviane Reding, 'Digital Sovereignty: Europe at a Crossroads' (2016) <https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf >. For an overview of the discourse on digital sovereignty see Rocco Bellanova, Helena Carrapico & Denis Duez, 'Digital/sovereignty and European security integration: an introduction', (2022) 31 European Security 337, 346-49; Georg Glasze et al., 'Reception and Elaboration of "Digital Sovereignty" in Three European Discourse Arenas: France, Germany, and the EU', (2023) 28 Geopolitics 928, 929-31; Stephane Couture & Sophie Toupin, 'What does the notion of "sovereignty" mean when referring to the digital?', (2019) 21 New Media & Society 2305, 2312-13.

2 See, e.g., Thierry Breton, then Commissioner for Internal

its core, digital sovereignty is about the autonomous and effective control of digital technologies and services. In this vein, Ursula von der Leyen described European digital sovereignty as "*the capability that Europe must have to make its own choices, based on its own values, respecting its own rules*".[3] The ascent of digital sovereignty on the EU's political agenda has not been limited to the rhetoric of its officials. Rather, digital sovereignty can be seen as the guiding normative ideal of the EU's approach to regulating data, digital technologies, and online activities. Although only few proposals and legislative acts explicitly reference the notion of digital sovereignty, the goals of extending EU values, laws, and norms to the digital space and strengthening the EU's autonomous control over online activities underlie a wide range of legislative acts.

2 The EU's recent embrace of digital sovereignty contrasts sharply with the internet's traditional self-understanding as a global space of freedom where, according to John Perry Barlow's famous Declaration of the Independence of Cyberspace, states would exercise no sovereignty and their legal systems would not apply.[4] State Sovereignty and the digital space were thought to be incompatible. Whereas state sovereignty would require effective and monopolized control over a bounded territory, the digital space was to be borderless, global, and characterized by horizontal power relations.[5] In reality, the digital space was never as independent from state interference as cyber-libertarians envisioned it to be. States have always used their control of the internet's underlying physical infrastructures to regulate the online activities of individuals and organizations in order to, for example, steer the exchange of communication and data or protect intellectual property rights.[6] Nevertheless, the degree of control that states in the West have exercised over the digital space could justifiably be described as relatively weak.[7] Due to the fast pace of digital innovation and the economic and social promises of a global internet, European and North American countries were reluctant to interfere too strongly with the organization of the digital space through private actors.[8] Against this background, the EU's embrace of digital sovereignty as a normative ideal represents the culmination of a paradigm shift away from supporting an open internet that is based on liberalized markets and transnational connectivity towards a regulatory approach that intervenes more actively in the organization of the digital space.

3 The EU's new emphasis on digital sovereignty is motivated by a perceived loss of its autonomy, competitiveness, and security in the digital space.[9]

Market, 'Speech at Hannover Messe Digital Days' (July 15, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/speech_20_1362>; Charles Michel, then President of European Council, 'Speech at "Masters of digital 2021": Digital sovereignty is central to European strategic autonomy' (Feb. 3, 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event>; European Parliament Research Service, 'Digital Sovereignty for Europe' (2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf>; Programme for Germany's Presidency of the Council of the European Union, 'Together for Europe's recovery' (2020) 8 <https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf>.

3 Ursula von der Leyen, 'Shaping Europe's digital future' (Feb. 19, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260>.

4 See John P. Barlow, 'A Declaration of the Independence of Cyberspace' (Feb. 8, 1996) <https://www.eff.org/cyberspace-independence>; see further Edoardo Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives' in Federico Fabbrini, Edoardo Celeste & John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (2021) 211, 214.

5 Celeste (n. 4), 212; Thorsten Thiel, 'Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation' in Jeanette Hofmann, Norbert Kersting, Claudia Ritzi & Wolf J. Schünemann (eds), *Politik in der digitalen Gesellschaft: zentrale Problemfelder und Forschungsperspektiven* (2019) 47, 48.

6 Celeste (n. 4), 214; Jack Goldsmith & Tim Wu, Who controls the Internet? (2006) 65-85; Julia Pohle, Digital Sovereignty. A new key concept of digital policy in Germany and Europe (2020) 9; Thiel (n. 5), 48-49.

7 In contrast, digital sovereignty has been an integral part of the digital policies of many (autocratic) states, notably China and Russia, for many years; see, e.g., Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realisation' in Dennis Broeders & Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 107, 115; Anqi Wang, 'Cyber Sovereignty at its boldest: A Chines Perspective', (2020) 16 Ohio St. Tech. L.J. 395; Lizhi Liu, 'The Rise of Data Politics: Digital China and the World', (2021) 56 Studies in Comparative International Development 45; Louis Pétiniaud et al., 'Russia's Pursuit of "Digital Sovereignty": Political, Industrial and Foreign Policy Implications and Limits', (2023) 28 Geopolitics 924, 925.

8 For an analysis of the German discourse of the 1990s and 2000s on online state interventions see Finn Dammann & Georg Glasze, '"Wir müssen als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen!" Historische Rekonstruktion und internationale Kontextualisierung der Diskurse einer "digitalen Souveränität" in Deutschland' in Georg Glasze, Eva Odzuck & Ronald Staples (eds), *Was heißt digitale Souveränität?* (2022) 29, 31-35.

9 The terms digital space and cyberspace are used interchangeably and understood broadly in this Article.

There are valid concerns that European values and the European legal, moral, and economic order have been undermined in cyberspace. This development has been attributed primarily to the dominant positions of powerful digital platforms within the economic and social spheres of the digital space. The predominantly American platform operators, in particular Meta, Apple, Alphabet, Amazon, and Microsoft, are considered to hold "*de facto sovereignty*".[10] They own essential digital infrastructures and, as *private legislators*, set important rules for social and economic interactions in the digital space.[11] Because of their infrastructural and quasi-legislative power, large digital platforms are able to steer the trajectory of the digital space, perform quasi-governmental functions of market regulation, and shape social and economic interactions on the internet in a way that can conflict with the EU's values and interests.[12]

4 Furthermore, from a foreign policy and security perspective, serious threats to Europe's cybersecurity and political order emanate from hostile states and other malicious actors. Cyberattacks pose a threat on multiple levels: they can violate citizens' privacy, harm the European economy through business sabotage or espionage, and disrupt the functioning of government services and critical infrastructures.[13] State-sponsored disinformation, initiated in particular by Russia, is spread through digital channels and can distort public discourse and undermine fair elections.[14] In addition, there is the widespread economic concern that Europe suffers from a lack of digital competitiveness and technological self-sufficiency.[15] Digital innovation may threaten the future success of Europe's traditionally strong but slow-to-adapt industrial sector and it is feared that Europe will be left behind, as the majority of digital cutting-edge technologies and services, including Artificial Intelligence (AI), are funded and developed outside of the EU.[16] These developments may jeopardize Europe's economic welfare and lead to a precarious dependency on foreign businesses.[17] In the long-term, this dependency could undermine sovereignty goals relating to Europe's cybersecurity and its regulatory and geostrategic autonomy.[18]

5 This Article explores how the EU is reacting against these threats by promoting its digital sovereignty through legislation. To this end, the Article aims to develop a coherent and analytically useful definition of digital sovereignty based on traditional political and legal understandings of the concept of state sovereignty (**B.**). This definition serves to distinguish the EU's digital sovereignty from other related concepts that are also sometimes discussed under the notion of digital sovereignty, i.e., Europe's technological independence, on the one hand, and the autonomous control of individuals and private organizations over their data, on the other hand. Based on a clear understanding of the concept of digital sovereignty, the Article proceeds by outlining through which legal acts and for which purposes the EU has promoted its digital sovereignty and technological independence (**C.**). The Article concludes with a high-level evaluation of the quest

Following Milton Mueller, the digital space is defined here as "*the virtual space for interaction created by joint use of compatible data communication protocols*"; see Milton Mueller, 'Against Sovereignty in Cyberspace', (2020) 22 International Studies Review 779, 788. This digital space is made up of infrastructures, technologies, and data, and includes all online content, online activities, and online interactions among humans and between humans and computers; see Benjamin Peters, 'Digital' in Benjamin Peters (ed), *Digital Keywords* (2016) 93, 94.

10 Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', (2020) 33 Philosophy & Technology 369, 372.

11 Julia Pohle & Thorsten Thiel, 'Digital sovereignty', (2020) 9 Internet Policy Review 1, 4;, at 6-7; Pohle (n. 6), 7; Ulrich Dolata, 'Plattform-Regulierung: Koordination von Märkten und Kuratierung von Sozialität im Internet', (2019) 29 Berliner Journal für Soziologie 179, 194; Jacques Crémer et al., Competition policy for the digital era (2019) 60-63.

12 Floridi (n. 10), 372; Dolata (n. 11), 194.

13 Matthias Bauer & Fredrik Erixon, 'Europe's Quest for Technological Sovereignty: Opportunities and Pitfalls', (2020) ECIPE Occasional Paper No. 02/2020, 26 <https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf>; Lokke Moerel & Paul Timmers, *Reflection on Digital Sovereignty* (2021), 9 <https://ssrn.com/abstract=3772777>.

14 Richard A. Clarke, 'Hostile State Disinformation in the Internet Age', (2024) 153 Daedalus 45, 45-56; Andrew M. Guess & Benjamin A. Lyons, 'Misinformation, Disinformation, and Online Propaganda' in Nathaniel Persily & Joshua Tucker (eds), *Social Media and Democracy* (2020) 10, 13-16.

15 European Parliament Research Service (n 2), 2.

16 Bauer & Erixon (n. 13), 13; Benjamin Farrand & Helena Carrapico, 'Digital Sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity', (2022) 31 European Security 435, 448; European Parliament Research Service (n 2), 2.

17 For a comprehensive overview of, e.g., Germany's technological dependencies see Bundesministerium für Wirtschaft und Energie, *Schwerpunktstudie Digitale Souveränität* (2021) 15-30 <https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6>.

18 See also Bellanova, Carrapico & Duez (n. 1), 348; Dammann & Glasze (n. 8), 48; Moerel & Timmers (n. 13), 11; Linda Monsees & Daniel Lambach, 'Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity', (2021) 31 European Security 377, 379.

for digital sovereignty and discusses some of its pitfalls (**D.**).

B. The Concept of Digital Sovereignty

6 Calls for strengthening Europe's digital sovereignty raise a variety of different issues that are to some extent interrelated, but address different actors and require different solutions.[19] They can refer to the control exercised by individual citizens and private organizations over their data, the ability of the EU and its Member States to autonomously govern cyberspace and to ensure cybersecurity, or the technological independence of the European economy. Furthermore, the term digital sovereignty is used in political and academic discourses for a variety of other claims, notions, and narratives, which are not related to the EU.[20] The discursive versatility of the term digital sovereignty and its intuitive applicability to different subject matters contribute to its popularity as a catch-all term.[21] Yet, the widely divergent uses of the term complicate analyses of the content of claims about digital sovereignty and their justifications.[22]

7 For the sake of conceptual and analytical clarity, it is therefore necessary to untangle different notions and meanings and to define digital sovereignty in a way that differentiates it from other (related) concepts.[23] In particular, the concept of digital sovereignty shall be delineated from the concepts of individual and organizational data autonomy and of Europe's technological and economic independence, which are also frequently discussed under the heading of European digital sovereignty.

I. Individual and Organizational Data Autonomy

8 The terms digital sovereignty or data sovereignty are sometimes used to refer to the autonomous control of individuals or private organizations over "their" data.[24] This individual digital (or data) sovereignty is typically understood to refer to the "*abilities and possibilities of individuals and institutions to be able to exercise their role(s) in the digital world independently, self-determinedly and securely*".[25] Using the term digital (or data) sovereignty to refer to the concepts of factual self-determination and autonomy of individuals is, however, misleading. For one, it is contrary to traditional legal and political understandings of sovereignty, which refer to the autonomy and control of states.[26] The same is true with regard to the discourse on digital sovereignty, in which digital sovereignty is predominantly understood to refer to state power and control in the digital space and the term data sovereignty typically refers to the state's control over data flows and is most coherently viewed as an element of the state's digital sovereignty.[27] Furthermore, individual data sovereignty has misleading connotations as the term sovereignty seems to imply an individual's legal or moral *right* to control their data.[28] Yet, according to the most wide-spread definitions, individual data sovereignty only refers to the *de facto control* exercised by individuals or organizations over the collection, use, and sharing of their data. Therefore,

19 This Section builds on Lukas von Ditfurth, *Datenmärkte, Datenintermediäre und der Data Governance Act* (2023) 193-201.

20 For in-depth analyses of the discourse about digital sovereignty see Couture & Toupin (n. 1); Patrik Hummel et al., 'Data sovereignty: a review', (2021) Big Data & Society 1, 2; Daniel Lambach & Kai Oppermann, 'Narratives of digital sovereignty in German political discourse', (2023) 36 Governance 693.

21 Lambach & Oppermann, (n. 20), 705; Dammann & Glasze (n. 8), 50.

22 See also Hummel et al. (n. 20), 2.

23 The Article's aim is not to interpret the use of the term by EU officials in speeches, but to develop a coherent and analytically useful concept of digital sovereignty based on traditional and established academic understandings of the term.

24 See, e.g., Pohle & Thiel (n. 11), 11; Pohle (n. 6), 16; Steffen Augsberg & Petra Gehring, Datensouveränität: Positionen zur Debatte (2022); Clara Beise, 'Datensouveränität und Datentreuhand', (2021) Recht Digital [RDi] 597; Alexander Roßnagel, 'Digitale Souveränität im Datenschutzrecht', (2023) Multimedia und Recht [MMR] 64.

25 Gabriele Goldacker, *Digitale Souveränität* (2017) 3 <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>.

26 See also Christian Rückert et al., 'Souveränität, Integrität und Selbstbestimmung: Herausforderungen von Rechtskonzepten in der digitalen Transformation' in Georg Glasze, Eva Odzuck & Ronald Staples (eds), Was heißt digitale Souveränität? (2022) 159, 160.

27 Couture & Toupin (n. 1), 2313; Anupam Chander & Haochen Sun, 'Sovereignty 2.0', (2023) 55 Vand. J. Transnat'l L. 283, 294.

28 For example, Gerrit Hornung and Sabrina Schomberg see a close parallel between the term data sovereignty and the right to informational self-determination as developed by the German Constitutional Court, see Gerrit Hornung & Sabrina Schomberg, 'Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Data Governance Acts', (2022) Computer und Recht 508, 510.

it is more accurate to refer to the data autonomy of individuals and organizations instead of their digital or data sovereignty.

II. Digital Sovereignty

9 At its most abstract level, digital sovereignty is defined here as state sovereignty in the digital space.[29] In order to flesh out this abstract definition, this Section will first briefly explore the well-established understanding of state sovereignty in jurisprudence and political science and then extend it to the digital space.

1. Dimensions of State Sovereignty

10 Although sovereignty is a shifting concept that has taken on many different shades over the course of centuries[30], there has remained a core meaning of the concept which still serves "*as the chief organizing principle of the international states system*".[31] At its core, sovereignty is defined as supreme authority within a territory.[32] This supreme authority is traditionally (and still today) held and exercised by the state. The core definition of sovereignty can be broken down into different facets and elements, some of which are central to the concept of digital sovereignty. On a fundamental level, an important distinction is to be made between the sovereignty *within* the state and the sovereignty *of* the state.[33]

11 As sovereignty within the state refers to the organization of authority within a political community[34], it is only the sovereignty of the state that is relevant to the concept of digital sovereignty. The sovereignty of the state can be divided into three separate but related dimensions: its internal sovereignty, its external sovereignty, and its legal sovereignty under public international law. The internal sovereignty of the state manifests itself in the ability and authority of the state to set binding legal rules for its subjects on its territory and to enforce them effectively by means of its monopoly on the use of force.[35] This internal sovereignty is composed of two essential elements – control and authority. Control refers to the actual ability or power of the state to direct and determine activities and developments within its territory.[36] Authority is the mutually recognized *right* of an actor to set rules, to command and to be obeyed.[37] This way, a state's sovereignty is to some extent linked to the legitimacy of state and government.[38]

12 External sovereignty refers to the exclusion of foreign states from interfering with the control and authority of a state within its territory.[39] Internal and external sovereignty are two sides of the same coin; each presupposes the other.[40] At its core, external sovereignty is the basis for the existing international order, in which "*states exist in specific territories, within which domestic authorities are the sole arbiters of legitimate behavior*".[41] External sovereignty is lost when a state relinquishes its supreme control and authority over a territory to a foreign actor, for example, through foreign intervention or voluntary invitation.[42]

13 International legal sovereignty is based on the recognition of states.[43] Generally, the sovereignty

29 Similarly, Anupam Chander and Haochen Sun understand the term digital sovereignty "to mean the application of traditional state sovereignty over the online domain", see Chander & Sun (n. 27), 292.

30 For a comprehensive historical account see generally Francis H. Hinsley, *Sovereignty* (2d edn, 1986).

31 Daniel Philpott, 'Sovereignty' in George Klosko (ed), *The Oxford Handbook of the History of Political Philosophy* (2011) 561, 561.

32 Ibid; Samantha Besson, 'Sovereignty' in *Max Planck Encyclopedias of International Law* (2011) para. 1 <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=MPIL>.

33 Albrecht Randelzhofer, '§ 17 Staatsgewalt und Souveränität' in Josef Isensee & Paul Kirchhof (eds), Handbuch des Staatsrechts II (3rd edn, 2004) 143, 145 para. 4; Christian Hillgruber & Hans Otto Seitschek, 'Souveränität' in Görres-Gesellschaft (ed) Staatslexikon V (8th edn, 2021).

34 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (1999) 11. It was this dimension of sovereignty and the questions of who the absolute sovereign is and ought to be, which the early theorists of sovereignty, in particular Jean Bodin and Thomas Hobbes, were primarily concerned with.

35 Randelzhofer (n. 33), 160 para. 39; Hillgruber & Seitschek (n. 33); Enrico Peuker, Verfassungswandel durch Digitalisierung (2020) 197.

36 Krasner (n. 34), 12.

37 Krasner (n. 34), 10; Robert P. Wolff, *In Defense of Anarchism* (2nd edn, 1998) 2.

38 Philpott (n. 31), 561; Huw Roberts et al., 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', (2021) 10 Internet Policy Review 1, 6.

39 Philpott (n. 31), 563; Krasner (n. 34), 20; Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (7th edn, McGraw-Hill 2006) 319-20.

40 Randelzhofer (n. 33), 154 para. 24; Philpott (n. 31), 563; Besson (n. 32), para. 73; Robert Jackson, Sovereignty: the evolution of an idea (2007) 12.

41 Krasner (n. 34), 20.

42 Krasner (n. 34), 20; Morgenthau, (n. 39), 319-26.

43 Krasner (n. 34), 14. Public international law enshrines the sovereignty of states. According to Article 2(1) of the UN Charter, the UN is based on the principle of the sovereign equality of all its members.

of a state under public international law presupposes its internal and external sovereignty.[44] Nevertheless, this relation between international legal sovereignty and the actual control exercised by a state over its territory is fickle. In the past, states that had little actual control over their internal affairs have been recognized as sovereign states under public international law.[45]

2. State Sovereignty in the Digital Space

14 The traditional concept of state sovereignty can be applied to the digital realm. Accordingly, digital sovereignty is to be understood as state sovereignty in the digital space. To the concept of digital sovereignty, both the internal and external dimensions of state sovereignty are relevant. For a state to be fully digitally sovereign, two conditions must be met. First, the state must have the authority and control to autonomously shape the rules of the digital space within its territory. It must have the right and ability to set its own autonomous rules for all online activities and developments that take place within or directly affect its territory, rather than being subject to external rules set by foreign states or private organizations. Second, the state must be able to effectively uphold and enforce the rules it has established within its territory and to keep foreign states from interfering with its control. It must have the *de facto* power to ensure that by and large its laws are respected in the digital space insofar as its own physical territory is concerned.

15 Digital sovereignty thereby complements the traditional or analogue sovereignty of states.[46] It is one element of full state sovereignty in the digital age.[47] Since the supreme authority and control over a territory nowadays also requires authority and control over the online activities occurring within or directly affecting this territory, there is no tension between the traditional concept of sovereignty rooted in the territory of the state and its modern counterpart of digital sovereignty.[48] On the contrary, the notion of digital sovereignty is still tied directly to a state's territory. Digital sovereignty refers to the authority and control over online activities that either originate in the state's territory or that affect persons, organizations, or infrastructures within the state's territory.

16 There are two main objections leveled against this and similar understandings of digital sovereignty. First, one could argue that sovereignty applied to the digital space must be fundamentally different from traditional understandings, as the sovereignty of states is *de facto* shared with private organizations, which have gained control over essential activities and infrastructures of the digital space.[49] Although it is true that some digital platforms have attained extraordinary economic and social power in the digital space, this claim is unconvincing. No private company in the digital space holds the supreme authority and control required to qualify as sovereign. In the digital space, states continue to set authoritative laws for their people and no private company has been recognized as having such authority, i.e., the *right* to command and be obeyed.[50] Furthermore, sovereignty not only requires a great amount of control over a (digital) territory, rather it requires that the sovereign's authority and control is the highest.[51] As, for example, the severe restrictions imposed on foreign digital companies in China and Russia as well as the US law aimed at banning TikTok have shown, the supreme authority over their digital territories still lies with states, not with private organizations.[52]

17 The second objection is raised against the very possibility of state sovereignty in the digital space. According to Milton Mueller, no state actor can have the monopoly on force over all of cyberspace to be considered sovereign.[53] Rather, there is only a shared global cyberspace and states can merely leverage their sovereignty over actors and infrastructures in their territory to influence the use of certain sites or applications.[54] Although it is true that supreme authority over the entire global digital space cannot realistically be achieved by a single state, it does not follow that the complete rejection of the concept

44 Randelzhofer (n. 33), 154 para. 25; Martin Nettesheim, '§ 5 Die Souveränität' in Klaus Stern, Helge Sodan & Markus Möstl (eds), Das Staatsrecht der Bundesrepublik Deutschland I (2nd edn, 2022) 261, 273 para. 37.

45 Krasner (n. 34), 15-16.

46 Floridi (n. 10), 375.

47 See also Hummel et al. (n. 20), 7.

48 Chander & Sun (n. 27), 291.

49 See, e.g., Luciano Floridi's claim that "corporate digital sovereignty" is a "political reality", Floridi (n. 10), 373; see also Anna Tiedeke, 'Die (notwendige) Relativität digitaler Souveränität', (2021) Multimedia und Recht [MMR] 624, 626.

50 See also Huw Roberts, 'Digital Sovereignty and Artificial Intelligence: A Normative Approach', (2024) 70 Ethics and Information Technology 1, 6-8.

51 Philpott (n. 31), 561-62.

52 See also Andrew K. Woods, 'Litigating Data Sovereignty', (2018) 128 Yale L.J. 328, 360-63 ; Thiel (n. 5), 52-53; Ciaran Martin, 'Geopolitics and Digital Sovereignty' in Hannes Werthner, Erich Prem, Edward A. Lee & Carlo Ghezzi (eds), Perspectives on Digital Humanism (2022) 227, 229. As Jack Goldsmith and Tim Wu already emphasized in 2006, governments are able to exercise control over the internet through their control of the physical infrastructures underlying the network within their borders, see Goldsmith & Wu (n. 6), 50-58, 65-85.

53 Mueller (n. 9), 790.

54 Mueller (n. 9), 790.

of digital sovereignty is necessary or appropriate. The usefulness and timeliness of the concept of digital sovereignty derives from its suitability for capturing the current efforts of states to control digital activities emanating from and affecting their territories. It is neither necessary nor useful to define the concept of digital sovereignty, as Milton Mueller does, in a way that is wholly detached from states' territories.[55] Instead, the term digital sovereignty can reasonably be used to refer to the authority and control that a state exercises over its domestic digital space or territory, i.e., over the online activities of persons within its geographical territory and over online activities originating from third countries that directly affect persons, organizations, and objects located within the territory of the EU. Such activities include, for example, the provision of foreign digital services in the EU, the posting and publishing of online content accessible from within the EU, and data flows to and from servers located in the EU.

3. Digital Sovereignty of the EU

18 Applying the concept of digital sovereignty to the EU raises the unresolved question of whether and how the EU itself can be (digitally) sovereign. After all, the effects of the European integration on the sovereignty of the EU and its Member States are complex and controversial.[56] Whereas, for example, the German Constitutional Court rejects the notion of a sovereign EU and assumes that all sovereignty continues to remain with the Member States[57], many European law scholars hold the view that sovereignty is in fact shared or pooled between the EU and its Member States.[58] For the purposes of this Article, the internal sovereignty relationship between the EU and the member states need not be explored further. In relation to the pursuit of European digital sovereignty against foreign states and private enterprises, the EU and its Member States can be regarded as a single entity. In this Article, European digital sovereignty will therefore be understood as the autonomous and effective exercise of sovereign power by EU institutions together with the Member States.

III. Technological and Economic Independence

19 Although related in practice, the technological and economic independence of a state or the EU is conceptually different from its (digital) sovereignty. After all, the authority of a sovereign state to enact and enforce laws of its own volition is not abrogated by *de facto* economic or technological dependencies.[59] As long as goods and services are autonomously and effectively regulated by a state, its sovereignty is not undermined by the fact that those goods and services are offered by foreign businesses.[60] Nevertheless, a lack of technological and economic independence can indirectly affect Europe's control over the digital space, just as it can lead to a loss of economic prosperity. For example, the presence of European tech companies could facilitate the enforcement of EU law, as authorities of the Member States have the legal authority to issue and execute legal orders against domestic companies on their territory. Besides, EU cybersecurity may benefit from more digital services provided from within the EU.

C. EU Legislation and the Quest for Digital Sovereignty

20 Full digital sovereignty, defined as the complete authority and ability of the EU and its Member States to autonomously shape the rules of the digital space within their territory and to effectively enforce those rules, represents an ideal state that is neither fully achievable in practice nor necessary for a state to be considered sovereign.[61] The possession of (digital) sovereignty is best understood as a gradual property and not as a binary property. Although the EU and its Member States still exercise a

55 Only if based on this understanding, would the concept of digital sovereignty denote something that is unachievable and contradictory.

56 See, e.g., Dieter Grimm, *The Constitution of European Democracy* (2017) 39-56.

57 According to the German Federal Constitutional Court, the Member States merely delegate individual (incomplete) state powers to the EU; see Bundesverfassungsgericht [Federal Constitutional Court], Jun. 30, 2009, 123 BVerfGE 267, 380-406; see also Ferdinand Wollenschläger, 'Artikel 23 GG' in Horst Dreier (ed), Grundgesetz Kommentar II (3rd edn, 2015), para. 88-93.

58 See John Peterson, 'The European Union: Pooled Sovereignty, Divided Accountability', (1997) 45 Political Studies 559; William Wallace, 'The Sharing of Sovereignty: the European Paradox', (199) 47 Political Studies 503; Lisa-Marie Lührs, 'Europäische Souveränität als mehrdimensionaler Rechtsbegriff', (2022) Europarecht [EuR] 673, 680; Utz Schliesky, *Souveränität und Legitimität von Herrschaftsgewalt* (2004) 507-586.

59 Morgenthau, (n. 39), 319-22.

60 Chander & Sun (n. 27), 310.

61 The claim that Europe's control over the digital space is weakened does not imply that it has lost its (digital) sovereignty (fully). As Rocco Bellanova et al. put it: "*Sovereignty is an unfulfilled political goal, insofar it is never truly absolute nor undisputed*", see Bellanova, Carrapico & Duez (n. 1), 340.

considerable amount of sovereignty over the digital space, there are valid concerns that Europe's digital sovereignty, specifically its control over the digital space, has been relatively weakened.[62] The objective of strengthening Europe's digital sovereignty refers to efforts to increase the relative level of control exercised by the EU and its Member States over the digital space. In particular, but not exclusively, the EU is seeking to strengthen its internal sovereignty, as it sees powerful private businesses as the main threat to its digital sovereignty.[63]

21 Although the term digital sovereignty is rarely mentioned explicitly in the EU's legislative acts[64], this Section will attempt to show that digital sovereignty can be regarded as an overarching objective and framework of EU digital policy that connects different EU legal acts.[65] This approach is consistent with recent findings that there have been broad shifts in EU digital policy towards more autonomy and control, even if the language of digital sovereignty has not been used to the same extent in all relevant policy sub-areas.[66] Based on the definition of digital sovereignty developed above, it will be outlined how the EU attempts to autonomously (re-)shape the rules of the digital space through legislation (**I.**). Subsequently, the EU's efforts to improve its legal enforcement mechanisms and to promote compliance with its laws in the digital space will be examined (**II.**). Furthermore, since the cybersecurity of the EU and its Member States is an important building block for Europe's internal and external sovereignty, the EU's measures to protect the cybersecurity of state institutions and critical infrastructures will be explored (**III.**). Finally, because they are closely related to the EU's pursuit of digital sovereignty and because EU institutions do not make as clear a distinction between digital sovereignty and technological independence as the definition above[67], key legal efforts to improve Europe's technological independence will be described briefly (**IV.**).

I. Shaping the Rules of the Digital Space

22 Central to the EU's quest for digital sovereignty are its efforts to re-shape the rules of the digital space in accordance with the European values and principles enshrined in Articles 2 and 3 of the Treaty on European Union (TEU).[68] Strictly speaking, these legislative efforts are themselves an exercise of the EU's digital sovereignty, as they are an instance of the EU using its authority to shape the rules of the domestic digital space. They are still included here as part of the EU's pursuit of greater digital sovereignty, because they are intended to align the rules of cyberspace more closely with the autonomous values and interests of the EU. By supplanting the informal digital order shaped by tech companies with formal legislation, these legislative efforts serve to extend the EU's autonomous control over its domestic cyberspace, thereby promoting the EU's digital sovereignty.

23 The values pursued by the EU include, in particular, the strong protection of individual human rights, the safeguarding of democracy, and the promotion of competition and fairness in digital markets. In view of the EU's legislative competencies, it is not surprising that these objectives are pursued primarily via the regulation of the single market.[69] There is a natural fit between this market-based regulatory approach and the EU's sovereignty objective, because the EU's attempts to re-shape the rules of digital space are primarily directed against the activities of powerful digital businesses and not against foreign states.[70] According to the European Commission, it is the informal digital order created by digital platforms that has led to harms for individual rights, democracy, and competition

62 In general, claims about the weakening of a state's sovereignty typically refer to a lack of control, not to a lack of authority, see Krasner (n. 34), 12.

63 Chander & Sun (n. 27), 307.

64 Only Recital 2 of the Chips Act explicitly mentions the enhancing of digital sovereignty as one of its objectives. There, digital sovereignty is understood as technological independence, see European Commission, Chips Act Explanatory Memorandum, COM(2022) 46 final, 4. The Explanatory Memorandum to the AI Act emphasizes the need for common action at Union level to "*protect the Union's digital sovereignty and [...] to shape global rules and standards*"; see European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 6.

65 This claim in no way implies that the strengthening of digital sovereignty is the only or primary objective of these legal acts.

66 Gerda Falkner et al., 'Digital Sovereignty – Rhetoric and Reality', (2024) 31 Journal of European Public Policy 2099.

67 See Theodore Christakis, 'European Digital Sovereignty, Data Protection, and the Push toward Data Localization' in Anupam Chander & Haochen Sun (eds), *Data Sovereignty* (2023) 371, 372.

68 Consolidated Version of the Treaty on European Union OJ C 202, 7.6.2016, 13. See also Celeste (n. 4), 221; Pohle (n. 6), 7.

69 Most legal measures discussed here are based on Article 114 TFEU, according to which the EU may adopt legal measures which have as their object the establishment and functioning of the internal market. This includes the DSA, DMA, DGA, DA, AI Act Proposal, and EMFA Proposal. In addition to Article 114 TFEU, the AI Act Proposal is also based on Article 16 TFEU. The GDPR is based exclusively on Article 16 TFEU.

70 Chander & Sun (n. 27), 307.

in Europe.[71]

1. Protecting Fundamental Rights

24 The EU's most fundamental goal is to build a human centered digital economy that respects individual human rights, in particular human dignity and privacy.[72] Cornerstone of this rights-based approach is still the General Data Protection Regulation (GDPR)[73], which predates von der Leyen's presidency and seeks to protect the personal data of natural persons within the EU in accordance with Article 8(1) of the Charter of Fundamental Rights of the EU (the Charter) and Article 16(1) of the Treaty on the Functioning of the EU (TFEU).[74] Building on the EU Data Protection Directive[75], the EU introduced the GDPR to respond to the rapid technological developments and the ever-increasing collection and sharing of personal data by implementing strong safeguards for the protection of personal data.[76] By establishing strict principles and narrow justifications for the processing of personal data, the GDPR restricts both the commercial exploitation of personal data and the unrestrained use of personal data for state surveillance purposes.[77] In particular, the GDPR seeks to counter the data capitalism of the digital economy, in which businesses profit from personal data at the expense of data subjects' privacy and their control over personal information.[78]

25 While the GDPR will remain the central regulation for protecting personal data for the foreseeable future, the EU has recently adopted complementary regulations aimed at increasing data protection levels within the EU. The Data Governance Act[79] shall set up a legal framework for data intermediaries to strengthen the control of data subjects over their personal data.[80] Furthermore, the Digital Services Act (DSA)[81] imposes special risk management obligations on so-called Very Large Online Platforms (VLOPs), which are intended to safeguard the privacy and other fundamental rights of individuals.[82] Both the GDPR and the DGA not only promote the EU's digital sovereignty but also strengthen the data autonomy of individuals to some extent.[83]

26 The regulation of Artificial Intelligence is the other main area where the EU is trying to establish a robust legal framework for protecting individual rights with the Artificial Intelligence Act (AI Act)[84].[85] Under the risk-based and multi-tiered approach of the AI Act, AI systems with unacceptable risks are fully prohibited, high-risk AI systems are subject to strict regulation, and low-risk systems must comply only with moderate obligations.[86] AI practices that are

71 European Commission, COM(2020) 66 final, 3, 5.

72 See, e.g., European Commission, COM(2020) 66 final, 4; Recital 4 GDPR; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 1.

73 Regulation (EU) 2016/679.

74 See Article 1(1) and (2) GDPR, Recitals 1 and 2 GDPR.

75 Directive 95/46/EC.

76 See only Recital 6 GDPR and Gerrit Hornung & Indra Spiecker gen. Döhmann, 'Introduction' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), *General Data Protection Regulation: Article-by-Article-Commentary* (2023) 1, 64 para. 195; see further on the history of EU data protection legislation and its objectives Orla Lynskey, *The Foundations of EU Data Protection Law* (2016) 47-75.

77 See Articles 5 and 6 GDPR as well as Recitals 39-50 GDPR.

78 On the notion of data or surveillance capitalism see further European Parliament Research Service (n. 2), 3; Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).

79 Regulation (EU) 2022/868.

80 See Recitals 5, 32, 38 DGA. See further Lukas von Ditfurth & Gregor Lienemann, 'The Data Governance Act: Promoting or Restricting Data Intermediaries?', (2022) 23 Competition and Regulation in Network Industries 270; Heiko Richter, 'Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing', (2023) 72 GRUR International 458; Gabriele Carovano & Michèle Finck, 'Regulating data intermediaries: the impact of the Data Governance Act on the EU's data economy', (2023) 50 Computer Law & Security Review 105830.

81 Regulation (EU) 2022/2065.

82 See Articles 34(1)(b) and 35 DSA as well as Recital 81 DSA.

83 The main examples of GDPR provisions aimed at promoting individual data autonomy include Articles 6(1)(a), 9(1), 13, 14, 16, 17, and 21 GDPR. However, the extent to which the GDPR promotes individual data autonomy should not be overstated. Neither the official objectives of the GDPR nor its main principles explicitly mention the self-determined control of data by the data subjects as a basic concern of the GDPR. Furthermore, the lawful processing of data does not necessarily require the consent of the data subject, but may also be based on, e.g., legitimate interests of the processor; see further Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?', (2021) 12 JIPITEC 246, 249-59; Opinion of Advocate General Campos Sanchez-Bordona, Case C-300/21 – UI v. Österreichische Post (Oct. 6, 2022), ECLI:EU:C:2022:756, para. 68-77.

84 Regulation (EU) 2024/1689.

85 Recitals 1, 2, 3, and 8 AI Act; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final,1; European Commission, COM(2020) 65 final, 1; Jonas Schuett, 'Risk Management in the Artificial Intelligence Act', (2023) European Journal of Risk Regulation 1, 5-6;. For a closer look at the risks posed by AI to the values of privacy and democracy see Karl Manheim & Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy', (2019) 21 Yale J.L. & Tech. 106.

86 See Recital 26 AI Act; European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 12; Schuett,

fully prohibited because of their negative impact on individuals and their rights include, for example, the use of AI systems that deploy subliminal techniques in order to materially distort a person's behavior in a manner that is likely to cause harm as well as AI systems that exploit the vulnerabilities of a specific group of persons due to their age or physical or mental disability.[87] AI practices that are considered to be high-risk due to their potential negative effects on individuals relate to, *inter alia*, the use of AI for determining access of natural persons to educational institutions, for making decisions on promotions and terminations of employees, and for evaluating the creditworthiness of natural persons.[88] Through these obligations, the AI Act is designed to protect the human dignity, autonomy, safety, and equality of natural persons from the intentional or negligent misuse of AI systems.[89]

2. Safeguarding Democracy

27 In keeping with its mandate under Article 3(1) TEU, the EU has introduced novel rules to protect the interrelated public values of democracy and media freedom and pluralism, which are threatened by foreign state interference as well as by content selection and display mechanisms of information intermediaries, such as social networks. The low costs of disseminating information on the internet and the lack of epistemic authorities controlling the accuracy of that information have enabled the spread of misinformation and disinformation, the latter sometimes being sponsored by hostile foreign states.[90] The spread of misinformation and disinformation has been acerbated by the inability or unwillingness of social networks to effectively stop the spread of false information on their platforms and their tendency to create filter bubbles and echo chambers around their users.[91] It is feared that these features of digital interaction have led to sharp increases in political manipulation and polarization that threaten the foundations of democracy.

28 In the absence of legislative foreign policy competences[92], the EU has used its internal market competence to impose due diligence obligations on VLOPs through the DSA in order to curb the spread of misinformation and disinformation and to reduce their potential for distorting democratic processes.[93] Providers of VLOPs, in particular social networks and search engines, need to carry out risk assessments for identifying any actual or potential negative effects on civil discourse and electoral processes stemming from the functioning of their service and its related systems.[94] If any relevant risks have been identified, the providers of VLOPs are under an obligation to put in place reasonable, proportionate, and effective mitigation measures specifically addressing these risks.[95] In addition, in the event of a crisis that poses a serious threat to public security or public health, the European Commission may order VLOPs to assess the impact of their services on the crisis and to take measures to mitigate that impact.[96]

29 The obligations of VLOPs under the DSA demonstrate

(n. 85), 4; David Bomhard & Marieke Merkle, Europäische KI-Verordnung: Der aktuelle Kommissionsentwurf und praktische Auswirkungen, (2021) Recht Digital [RDi] 276, 279.

87 See Article 5(1)(a) and (b) AI Act; see further Kalojan Hoffmeister, 'The Dawn of Regulated AI: Analyzing the European AI Act and its Global Impact', (2024) Zeitschrift für europarechtliche Studien [ZEuS] 182, 197-199.

88 Article 6(2) AI Act in conjunction with Annex III No. 3, 4, and 5. These high-risk systems are regulated strictly. For example, in order to minimize the risks of errors, biases, and discrimination stemming from technical inaccuracies of AI systems due to inaccurate training data or weaknesses of the underlying algorithms, Articles 9 and 10 AI Act require developers and users to establish a risk management system and to set in place appropriate data governance practices; see further Hoffmeister (n. 87), 202.

89 See Recitals 28, 31, 48, 59 AI Act.

90 On the lack of epistemic authorities on the internet see Brian Leiter, 'The Epistemology of the Internet and the Regulation of Speech in America', (2022) 20 Geo. J.L. & Pub. Pol'y 903, 918-921; on misinformation and disinformation see Andrew M. Guess & Benjamin A. Lyons, 'Misinformation, Disinformation, and Online Propaganda' in Nathaniel Persily & Joshua Tucker (eds), *Social Media and Democracy* (2020) 10.

91 For an overview see Luis Roberto Barrosoa & Luna van Brussel Barroso, 'Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth', (2023) 24 Chi. J. Int'l L. 51, 56-61. The extent to which filter bubbles and echo chambers actually exist is heavily debated. For an overview of the current state of research *see* generally Pablo Barbera, 'Social Media, Echo Chambers, and Political Polarization' in Nathaniel Persily & Joshua Tucker (eds), Social Media and Democracy (2020) 34; Peter M. Dahlgreen, 'A critical review of filter bubbles and a comparison with selective exposure', (2021) 42 Nordicom Review 15.

92 See Article 24(1) TEU.

93 See Recital 9 DSA.

94 See Article 34(1)(b) DSA and Recitals 9, 82, and 104 DSA. Among others, the EU Commission has designated Facebook, YouTube, Instagram, and TikTok as VLOPs. For a critical assessment of the DSA's approach to fighting disinformation see Alain Strowel & Jean De Meyere, 'The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?', (2023) 14 JIPITEC 66, 71-77.

95 See Article 35(1) DSA.

96 See Article 36 DSA; see further Strowel & De Meyere (no. 92), 77.

the EU's willingness to implement a European approach to regulating speech on the internet vis-à-vis the mostly American VLOPs, whose moderation of content practices are influenced by the American legal culture and its emphasis on the strong protection of free speech.[97] Whereas the First Amendment of the US Constitution imposes strict limits on the regulation of the content of speech, including for many types of false speech, the European legal culture is more open to regulating speech as the freedom of expression is not considered an absolute right and may be limited for reasons of public interest.[98]

30 The regulation of VLOPs under the DSA is complemented by the European Media Freedom Act (EMFA).[99] With the EMFA, the EU aims to protect media freedom and plurality from restrictions by Member States, but also from certain risks resulting from the increasing dependencies of media outlets on online information intermediaries.[100] Indirectly, the EMFA contributes to the protection of democracy, as media services perform important democratic functions as reliable news sources and public watchdogs.[101] The EMFA complements the DSA by regulating the treatment of certain independent and credible media services by VLOPs. It seeks to preserve media freedom and plurality by protecting independent media providers from deliberate and inadvertent abuses of the position of VLOPs as important gateways to journalistic content.[102] In particular, VLOPs must be transparent in their decisions to suspend their intermediation services with respect to content provided by such media service providers and they must remove any unjustified restrictions or suspensions.[103]

3. Promoting Fairness and Competition in Digital Markets

31 The EU has further adopted important legislation to promote European ideals of market fairness and competition in increasingly concentrated digital markets, including data markets. Whereas the Digital Markets Act (DMA)[104] imposes *ex ante* regulation on digital platforms that act as gatekeepers in already important digital markets, the DGA and the Data Act (DA)[105] regulate different aspects of the nascent European data economy in order to enable the emergence of well-functioning data markets.

32 The DMA targets the multi-dimensional power positions of the major digital platforms that supposedly constitute a threat to Europe's consumers and its lagging digital economy. In particular, the DMA reacts to the competition risks posed by the strong positive economies of scale and network effects of digital platform markets.[106] In combination with certain unfair practices employed by the providers of large and important digital platforms (gatekeepers), these effects have undermined the contestability and fairness of markets for certain crucial digital services, so-called core platform services.[107] These core platform services include,

97 Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', (2018) 131 Harv. L. Rev. 1598, 1618-1622.

98 Ioanna Tourkochoriti, 'The Digital Services Act and the EU as the Global Regulator of the Internet', (2023) 24 Chi. J. Int'l L. 129, 131-32. On the protection of false speech under the First Amendment see Leslie G. Jacobs, 'Freedom of Speech and Regulation of Fake News', (2022) 70 Am. J. Comp. L. 278, 280-86: Erwin Chemerinsky, 'False Speech and the First Amendment', (2018) 71 Okla. L. Rev. 1. Under EU law, limitations imposed on the right to freedom of expression pursuant to Article 11 of the Charter and Article 10(1) of the European Convention on Human Rights are permissible, if they are proportionate and necessary to fulfill certain objectives of public interest; see Lorna Woods, 'Art 11 – Freedom of Expression and Information' in Steve Peers, Tamara Hervey, Jeff Kenner & Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, 2021), para. 11.59 et seq.

99 Regulation (EU) 2024/1083.

100 See Recitals 2, 3, and 18 EMFA. The EMFA's shall contribute to the upholding of Article 11(2) of the Charter, according to which, the freedom and pluralism of the media are to be respected.

101 See Recitals 1, 40; European Commission, EMFA Explanatory Memorandum, COM/2022/457 final, 6; European Commission, COM(2020) 790 final, 11.

102 See Recitals 3, 50, and 55 EMFA.

103 Article 17(4) and (6) EMFA.

104 Regulation (EU) 2022/1925.

105 Regulation (EU) 2023/2854.

106 See Recital 2 DMA. For an overview of the competitive issues raised by these characteristics of platform markets see generally Stigler Committee on Digital Platforms, *Final Report* (2019), 34-43 <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf>; and Geoffrey Parker, Georgios Petropoulos & Marshall Van Alstyne, *Digital Platforms and Antitrust*, (2020) Bruegel Working Paper 06/2020 <https://www.bruegel.org/sites/default/files/wp_attachments/WP-2020-06-1.pdf>.

107 See Recitals 2 and 15 DMA. Gatekeepers are the providers of core platform services which meet certain qualitative and quantitative criteria and have been designated as such by the EU Commission, see Article 3 and Recitals 15 and 16 DMA. To date, the EU Commission has designated as gatekeepers Alphabet (Google), Amazon, Apple, ByteDance, Meta (Facebook), Microsoft, and Booking.com; see European Commission, 'Digital Markets Act: Commission designates six gatekeepers' (Sep. 6, 2023) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328>;

inter alia, search engines, social networks, web browsers, and video-sharing platforms.[108] Due to the lack of contestability and fairness on these core platform markets, their (competitive) functioning is impaired to the detriment of prices, quality, and innovation in the digital sector.[109] It is the goal of the DMA to ensure and restore the contestability and fairness of core platform markets by placing *ex ante* obligations on the provision of core platform services by gatekeepers.[110] These obligations correspond to certain practices of gatekeepers which are seen as harmful.[111] Obligations aimed at improving the contestability and fairness of core platform markets include, *inter alia*, restrictions on the data collection practices of gatekeepers, data access rights for end users and business users, and rules aimed at enabling the switching and multi-homing of end users and business users.[112]

33 The DGA is another piece of legislation that seeks to ensure competition and fairness on digital markets. While its primary goal is to promote trust in data intermediation services in order to facilitate the emergence of functioning data markets[113], the DGA also aims to ensure that data intermediation services will be provided in a competitive and fair environment.[114] The EU is determined to prevent undesirable market developments at an early stage by introducing a strict *ex ante* regulation for data intermediaries.[115] Hence, the DGA is designed to protect vertical and horizontal competition on data intermediation markets and to fend off the entry and domination of data intermediation markets by already powerful digital conglomerates.[116] In addition, data markets are to be regulated by the DA, which sets rules for the fair access to data generated by the use of products connected to the internet and for the invalidity of unfair contractual terms regarding the sharing of data.[117] Essentially, the DA seeks to empower the users of connected products and to spread the benefits derived from data generated by the Internet of Things more fairly.[118] In particular, manufacturers of connected products are obligated to make the data generated by the use of a connected product available to the respective product user free of charge.[119] These data can then be used by third parties to provide aftermarket or ancillary services.[120] Unlike the DMA and DGA, the DA is not aimed directly against the major digital platforms.[121] Rather, the DA addresses the lack of data sharing by manufacturers, many of which are European companies from traditional industry sectors.[122]

II. Effective Enforcement of European Law in the Digital Space

34 The EU further seeks to strengthen its digital sovereignty by improving its enforcement mechanisms to promote legal compliance in the

European Commission, 'Commission designates Booking as a gatekeeper' (May 13, 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2561>.

108 See Article 2(2) and Recitals 13 and 14 DMA.

109 See Recitals 3 and 4 DMA. Contestability refers to the presence of low market entry barriers as a condition for vigorous and dynamic inter-platform competition for core platform markets; see Recital 32 DMA and Jacques Crémer et al., 'Fairness and Contestability in the Digital Markets Act', (2023) 40 Yale J. on Reg. 101, 117-31. Unfairness is understood in the DMA as an imbalance in the bargaining power of gatekeepers and other market participants, which leads to an unfair and one sided distribution to gatekeepers of the benefits resulting from innovation and other efforts in core service markets; see Recital 33 DMA and Crémer et al., id., 108-17; Rupprecht Podszun et al., 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers', (2021) Journal of European Consumer and Market Law [EuCML] 60, 62.

110 See Articles 5(1) and 6(1) DMA. The DMA departs from traditional antitrust law approaches to regulation and instead relies on an ex ante regulatory approach similar to those for network industries; see Wolfgang Kerber, 'Taming tech giants with a per se rules approach? The Digital Markets Act from the "rules vs. standard" perspective', (2021) N° 3-2021 Concurrences 28; Podszun et al. (n. 109), 61.

111 See Recital 31 DMA.

112 See Articles 5 and 6 DMA and Recitals 36-64 DMA.

113 See infra Part C.IV.3.

114 See Recital 33 DGA; von Ditfurth & Lienemann (n. 80), 280-81.

115 For an extensive analysis see von Ditfurth (n. 19), 207-209 (2023).

116 von Ditfurth & Lienemann (n. 80), 288-90.

117 See Articles 3-13 DA. Other provisions of the DA related to the fair and pro-competitive regulation of the digital economy are the rules on switching between data processing services (Articles 23-31 DA), such as cloud services. For an analysis of the data access rights under the DA see Moritz Hennemann et al., *Data Act: An Introduction* (2024) 71-140.

118 See European Commission, Data Act Explanatory Memorandum, COM(2022) 68 final, 2-3; Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives', (2023) 72 GRUR International 120, 122.

119 See Articles 3 and 4 DA and Recitals 5, 6, and 20 DA.

120 See Recital 6 DA.

121 Nevertheless, the DA does include a mechanism to prevent that data access rights can be exploited by powerful digital platforms. According to Article 5(3) DA, product users may not request the sharing of the product data with undertakings that have been designated as gatekeepers under the DMA. Furthermore, gatekeepers may not oblige or incentivize product users to share their product data with them.

122 See Recital 2 DA; European Commission, SWD(2020) 295 final, 9-10; European Commission, SWD(2022) 34 final, 9-10.

digital space. Specifically, the EU is concerned with removing barriers to legal enforcement that are caused by distinctive features of the digital space, i.e., the transnational nature of cyberspace and the mobility of data. As a result of these features, the national territory as the physical place where states wield their authority has become less important for enforcing legally compliant online behavior. The EU has reacted to these developments by adopting legal measures aimed at improving European control over data access and global data flows (**1.**), extending the territorial scope of EU law (**2.**), requiring foreign organizations to designate representatives within the EU (**3.**), and obliging providers of digital platforms to regulate and moderate the content available on their platforms (**4.**).

1. Controlling Data Access and Data Flows

35 States have been struggling to control and monitor the (cross-border) movements of data for years. This issue has been exacerbated by increases in cloud usage for the storage of individual and organizational data.[123] Because of their mobility and divisibility, data are moved around in the cloud and stored in different server locations, including extraterritorial locations.[124] The global nature of the internet and the uptake of cloud usage have led to a situation where an individual or an organization and their data "*are now often separated by great distances and possibly several jurisdictions*".[125] Consequentially, a large amount of data held by EU citizens is located abroad which affects European law enforcement in two important ways. First, law enforcement agencies struggle to access data required as evidence for criminal proceedings.[126] Second, once data leave the jurisdiction of the EU and enter the jurisdiction of a third state, European agencies lack the effective means to ensure that third countries and private organizations comply with European legal rules.[127] The EU has taken legislative measures to address both of these issues.[128]

a.) Ensuring Access to Digital Evidence

36 The EU has adopted the E-Evidence Regulation[129] to ensure the effective access by Member States' law enforcement agencies to digital evidence stored in other EU and non-EU countries. The E-Evidence Regulation introduces an EU-wide legal framework for direct cooperation between judicial authorities in one Member State and digital service providers in another Member State, without actively involving the latter state.[130] Under certain conditions, the competent authorities of a Member State may directly order service providers offering their services in the EU to produce or to preserve certain electronic evidence data.[131] Service providers covered by the E-Evidence Regulation include, *inter alia*, instant messaging and email services as well as online marketplaces and hosting services provided via cloud computing.[132]

37 Importantly, the obligations to produce or preserve electronic evidence apply to service providers regardless of the location of the requested data as long as these data are related to services offered in the EU.[133] Thus, service providers may be required to hand over data to European law enforcement agencies that are located on servers in third countries. With

123 Woods (n. 52), 352. According to Statista, in 2022, 60% of worldwide corporate data were stored in the cloud, see <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data>.

124 Jennifer Daskal, 'The Un-Territoriality of Data', (2015) 125 Yale L.J. 326, 366-69.

125 Andrew K. Woods, Against Data Exceptionalism, 67 Stan. L. Rev. 729, 742 (2016); see also Daskal (n. 124), 373; Aude Géry & Florian Nicolai, 'Law Enforcement and Access to Transborder Evidence: the Quest for the Exercise of Digital Sovereignty?', (2023) 28 Geopolitics 941, 941-42.

126 Woods (n. 125), 739; Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective', (2022) 85 Modern Law Review 997, 1002-3; Géry & Nicolai, (n. 125), 941-42.

127 See with respect to the protection of personal data Peter Schantz, 'Article 44' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), *General Data Protection Regulation: Article-by-Article-Commentary* (2023) 775, 776 para. 4; Christopher Kuner, 'Article 44' in Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (2020) 755, 757.

128 The control exercised by a state over data flows within its borders and data flows from and to its territory is sometimes referred to as "data sovereignty", see Couture & Toupin (n. 1), 2312-13; Chander & Sun (n. 27), 293. In this Article, data sovereignty is understood to be just one aspect of the broader concept of digital sovereignty.

129 Regulation (EU) 2023/1543.

130 Theodore Christakis, *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive* (2023) 1-2 <https://ssrn.com/abstract=4306874>.

131 See Article 4 E-Evidence Regulation. The conditions for issuing evidence production orders or preservation orders are laid down in Article 5 and 6 E-Evidence Regulation respectively. Such orders may be issued for, e.g., the pursuit of criminal offences and must be necessary and proportionate. The orders may cover, inter alia, the production or preservation of IP data, traffic data, and content data, such as text, videos, or images.

132 See Article 2(4) E-Evidence Regulation and Recital 27 E-Evidence Regulation.

133 See Article 1 (1) and Recitals 21, 26 E-Evidence Regulation.

its extraterritorial reach, the E-Evidence Regulation mirrors the US CLOUD Act of 2018[134], which requires service providers to disclose all data in their control to US law enforcement agencies regardless of the location of the data.[135] Due to its extraterritorial reach, the E-Evidence Regulation will in many cases conflict with foreign laws. For example, the US Electronic Communications Privacy Act (ECPA) generally prohibits service providers from disclosing the content of electronic communications directly to foreign governments.[136] In order to minimize such conflicts, the E-Evidence Regulation provides for a judicial review procedure in cases where complying with evidence production orders would violate foreign laws.[137] However, even if there is an actual conflict between the E-Evidence Regulation and foreign laws, the courts of Member States may still decide to uphold the order to disclose evidence.[138] Thus, in case of conflict, the E-Evidence Regulation claims the primacy of EU law over foreign laws.

b.) Regulating International Data Transfers

38 Data transfers to third countries pose significant risks for the circumvention of the level of data protection under EU law, as there are few means available to European authorities to ensure compliance with EU law in foreign states. The EU and its Member States can only effectively control international data flows as long as the data is still on their territory.[139] Therefore, the EU has adopted legal rules to regulate international transfers of both personal and non-personal data. Most importantly, the GDPR governs the transfer of personal data to third countries.[140] Personal data may only be transferred to a third country, if the EU Commission has decided that the third country ensures an adequate level of data protection or if the controller or processor transferring the data has provided appropriate safeguards to guarantee the effective protection of data.[141] This way, the GDPR aims to ensure that the personal data of Europeans will enjoy a level of protection in third states that is essentially equivalent to that of the EU.[142]

39 With the adoption of the DGA and the DA, the EU has recently extended the regulation of international data flows to non-personal data. Both the DGA and the DA include similar statutes which restrict international transfers of non-personal data to third countries and the access of foreign governments to such data where such transfer or access would create a conflict with or contravene European law.[143] These provisions primarily aim to protect the trade secrets and intellectual property rights of businesses as well as national security interests of Member States.[144]

2. Extending the Territorial Reach of EU Law

40 The global and borderless nature of cyberspace poses another problem for the EU's sovereignty, as it allows digital services to be provided in the EU without the provider being established in the EU.[145] If EU laws merely apply to subjects within its own domestic territory, its rules could be easily circumvented by foreign actors who can offer their digital goods or services within the EU despite being established in third countries. The EU has addressed this potential regulatory gap by extending the scope of its legislation beyond its territory. It includes within the scope of its laws all persons who are active on its territory, regardless of whether they are established in the EU or in a third country. This extension of territorial scope is a key feature of the GDPR. Under its marketplace principle, the GDPR applies not only to data processing activities in the EU, but also to data processing activities by foreign entities that affect data subjects in the EU.[146] In doing so, the GDPR imposes obligations on data controllers and data processors, regardless of their actual geographic location or legal seat.[147] Mirroring

134 Clarifying Lawful Overseas Use of Data Act, contained in Consolidated Appropriations Act, 2018, PL 115-141, Division V.

135 Christakis (n. 130), 18. On the CLOUD Act see Stephen W Smith, 'Clouds on the Horizon: Cross-Border Surveillance under the US CLOUD Act', in Federico Fabbrini, Edoardo Celeste & John Quinn eds, Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (2021) 119.

136 See 18 U.S.C. § 2702(a)(3); Congressional Research Service, Cross-Border Data Sharing under the CLOUD Act (Apr. 23, 2018) 10-11) <https://www.everycrsreport.com/files/20180423_R45173_c8a82f6a7cee392e23453b5836546d6a68e5e779.pdf>.

137 Article 17 and Recitals 74-79 E-Evidence Regulation.

138 Article 17(6) E-Evidence Regulation.

139 Christoph Kuner, *Transborder Data Flows and Data Privacy Law* (2013) 105.

140 See Articles 44-49 GDPR.

141 See Articles 45 and 46 GDPR. For analyses of the GDPR regime for international data transfers see Leonie Wittershagen, *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit* (2022) 52-82; Tobais Naef, *Data Protection without Data Protectionism* (2022) 115-221.

142 See Recital 104 GDPR; Schantz (n. 127), 777 para. 6.

143 See Article 31(1) DGA; Article 32(1) DA.

144 See Recital 20 DGA and Recital 101 DA.

145 Adèle Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation', (2018) 9 JIPITEC 126, 127.

146 See Article 3(2) GDPR.

147 Stephan Koloßa, 'The GDPR's Extra-Territorial Scope: Data Protection in the Context of International Law and

the GDPR's approach, the marketplace principle has also been adopted for the DSA, DGA, DA, and AI Act.[148]

3. Requiring Representation of Foreign Providers of Online Services

41 A further mechanism used by the EU legislator to improve compliance with its rules is the requirement for international businesses to designate representatives within the EU territory.[149] Because of the global reach of the internet, it can be difficult to enforce obligations under EU law against foreign providers of digital services that do not have an establishment in the EU but are still subject to EU law due to the marketplace principle.[150] In particular, European authorities may struggle to communicate with foreign service providers and they lack the legal authority to deliver official orders on foreign territories.[151] Thus, the purpose of designating representatives is to promote the effectiveness and efficiency of information requests by European authorities. The designated representatives shall serve as points of contacts for all requests concerning the provision of their services within the EU and their compliance with EU law.[152]

4. Law Enforcement Responsibilities of Online Services

42 Online content can be easily and rapidly copied and shared over the internet. This characteristic enables mass infringements of intellectual property rights and personality rights. Since the early 2000s, there has been a large number of copyright infringements on the internet as a result of wide-spread file sharing practices.[153] In addition, the emergence of social media has been accompanied by an increase in the creation and dissemination of disinformation, misinformation, and online content that violates the personality rights of individuals or that can be classified as hate speech.[154]

43 Due to the large volume and rapid distribution of illegal online content, the effort required to monitor and prevent such legal violations exceeds the resources of law enforcement agencies. This situation has been exacerbated by the relatively liberal regulation of internet intermediaries in the EU and the US. Under the EU E-Commerce Directive[155] as well as the US Communication Decency Act[156] and the US Digital Millennium Copyright Act[157], online service providers were largely exempted from liability for illegal conduct of their users.[158] Partially departing from its traditionally liberal stance towards intermediary regulation, the EU has recently adopted legislation to improve online compliance by requiring certain internet intermediaries to ensure the legally compliant behavior of their users themselves. Thereby, the EU legislator is leveraging the *de facto* control exercised by powerful internet intermediaries over the digital space to improve the enforcement of EU law.

44 The DSA is the centerpiece of EU efforts to utilize digital service providers for law enforcement through mandatory self-regulation.[159] In principle,

Human Rights Law', (2020) 80 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht [ZaöRV] 791, 795; Gerrit Hornung, 'Article 3' in Indra Spiecker gen. Döhmann, Vagelis Papakonstantinou, Gerrit Hornung & Paul De Hert (eds), General Data Protection Regulation: Article-by-Article-Commentary (2023) 116, 155 para. 36.

148 See Article 2(1) DSA; Article 11(3) and Recital 42 DGA; Article 1(3) DA; and Article 2(1) AI Act. Other countries, including Japan and Brazil, have also adopted similar mechanisms for ensuring the extraterritorial applicability of their data protection laws; see, e.g., Article 75 of the Japanese Act on the Protection of Personal Information and Article 3 of the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais).

149 See Article 27 GDPR; Article 13 DSA; Article 11(3) DGA; Article 3 of Directive (EU) 2023/1544 (E-Evidence Directive).

150 See Recital 1 E-Evidence Directive; Schantz (n. 127), 776 para. 4.

151 Hannes Krämer, 'Extraterritoriale Wirkungen des Unionsrechts – eine normanalytische Skizze', (2021) Europarecht [EuR] 137, 144.

152 See Recital 80 GDPR and Recital 42 DGA.

153 See, eg., Felix Oberholzer-Gee & Koleman Strumpf, 'File Sharing and Copyright', (2010) 10 Innovation Policy and the Economy 10; Goldsmith & Wu (n. 6), 105-118.

154 See, e.g., Barrosoa & van Brussel Barroso, (n. 91), 56-61; Danielle K. Citron & Helen Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age', (2011) 91 B.U. L. Rev. 1435, 1447-1453; Majid Yar, 'A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media', (2018) 1 International Journal of Cybersecurity Intelligence & Cybercrime 5, 6-9. Typical personality rights include the right to privacy, the right to one's own image, and the prohibition of defamation, see Susanna Lindroos-Hovinheimo, 'Jurisdiction and personality rights – in which Member State should harmful online content be assessed?', (2022) 29 Maastricht Journal of European and Comparative Law 201, 204.

155 Directive 2000/31/EC.

156 47 U.S.C. § 230(c)(2).

157 17 U.S.C. § 512(g)(1).

158 For an in-depth analysis of online intermediary liability in the EU and the US see Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (2020).

159 Similar enforcement obligations are also present in Article 17(4) of the EU Digital Single Market Directive

the DSA retains the liability rules of the preceding E-Commerce Directive, according to which providers of online intermediary services are generally not legally responsible for third-party content, as long as they remain neutral intermediaries and are not aware of the potential illegality of the content.[160] However, the DSA introduces new and stricter procedural obligations for providers of hosting services and providers of online platforms, the latter being a sub-type of hosting services.[161] All providers of hosting services are required to put notice and action mechanisms in place, which allow third parties to inform them of the presence of illegal content on their services and enable the providers themselves to remove such content.[162] In addition, providers of online platforms must implement effective mechanisms and systems to handle internal complaints, to provide out-of-court dispute settlement for affected parties, and to cooperate with trusted flaggers of illegal content.[163] They are also required to suspend the provision of their services to users that frequently upload illegal content.[164] These obligations aimed at ensuring a legally compliant online environment are supplemented by additional obligations for VLOPs, which are obligated to conduct risk assessments to identify whether the dissemination of illegal content occurs through their services and whether their services have any negative effects on fundamental rights.[165] If such risks are identified, the VLOP providers must take effective mitigation measures, such as adapting their algorithmic recommender systems or adding to their content moderation personnel.[166]

III. Securing European State Institutions and Critical Infrastructures

45 The capacity of the EU and its Member States to effectively enforce their laws in cyberspace is an essential prerequisite for strengthening European digital sovereignty. This capacity requires the unimpaired functioning of state institutions and critical infrastructures, which are threatened by cyberattacks.[167] Cyberattacks are launched not only by cybercriminals but also by foreign states that engage in espionage and pseudo-military operations in cyberspace.[168] Hostile cyber activities by foreign states include, for example, large-scale infiltration and surveillance of government networks, power grid disruptions, and disruptions of public health services.[169]

46 The EU's approach to strengthening European cybersecurity is multi-pronged. It includes investments, policy, and legal instruments. One important policy instrument that specifically addresses the cybersecurity risks stemming from foreign technology providers is the 5G Toolbox. It is a set of non-binding recommendations for a common EU approach to ensuring the security of 5G networks in view of potential risks posed by the Chinese supplier Huawei.[170] In this regard, the promotion of Europe's cybersecurity crucially depends on the advancement of its technological independence.[171] On the legislative side, the EU

("upload filters") and Article 12 (j) DGA. On upload filters see Thomas Spoerri, 'On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market', (2019) 10 JIPITEC 173. On enforcement obligations under the DGA see von Ditfurth & Lienemann (n. 80), 287

160 See Articles 4-8 and Recital 17 DSA; Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation', (2021) 12 JIPITEC 361, 369; Martin Eifert et al., 'Taming the Giants: The DMA/DSA Package', (2021) 58 Common Mkt. L. Rev. 987, 1005-8.

161 See Recital 13 DSA. In particular, online platforms encompass social networks and online marketplaces. Other hosting services include cloud computing, web hosting, and file storage and sharing services, see Recital 29 DSA. For an overview over the layered obligations for special types of intermediary services (i.e. hosting services, online platforms, and VLOPs) see Buiten (n. 160), 368; Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules', (2024) 38 Berkeley Tech. L.J. 883, 900.

162 See Article 16 and Recitals 50-54 DSA. Pursuant to Article 17 DSA, they are further required to provide a specific statement of reasons to users affected by content takedowns or similar actions. See further Husovec (n. 161), 900-2; Eifert et al. (n. 160), 1009-13.

163 See Articles 20-22 and Recitals 58-62 DSA.

164 See Article 23 and Recital 64 DSA.

165 See Article 34(1)(a) and (b) and Recitals 80 and 81 DSA. See further Husovec (n. 161), 902-8.

166 See Article 35 and Recitals 87 and 88 DSA.

167 Roberts et al. (n. 38), 12; European Commission, JOIN(2020) 18 final, 4; see also Farrand & Carrapico (n. 16), 447.

168 See only Dennis Broeders & Bibi van den Berg, Governing Cyberspace: Behavior, Power, and Diplomacy in Dennis Broeders & Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 1, 1-2.

169 Lucas Kello, 'Cyber legalism: why it fails and what to do about it', (2021) 7 Journal of Cybersecurity 1, 9.

170 NIS Cooperation Group, Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (2020) <https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf>; European Commission, COM(2020) 50 final; European Commission, JOIN(2020) 18 final, 4. See further Monsees & Lambach (n. 18) 36, 384-86.

171 European Commission, COM(2020) 50 final; European Commission, JOIN(2020) 18 final, 11; NIS Cooperation Group (n. 170), 3.

has issued regulations and directives aimed at strengthening European cybersecurity in general and the cybersecurity of government institutions and critical infrastructures in particular. General measures include the Cybersecurity Act, which has fortified the role of the EU Agency for Cybersecurity (ENISA) and has established a security certification framework for digital products and services offered on the common market.[172] It is being complemented by the Cyber Resilience Act, which introduces horizontal cybersecurity requirements for all digital products and services in the EU.[173]

47 In addition, the EU has adopted legislative acts that are specifically aimed at improving the cybersecurity of EU institutions, Member State institutions, and critical infrastructures. The recent Cybersecurity Regulation requires the institutions, bodies, and agencies of the EU to establish internal cybersecurity risk management and control mechanisms.[174] The cybersecurity levels of the institutions and critical infrastructures of Member States are directly addressed by the NIS 2 Directive from 2022.[175] In particular, the NIS 2 Directive requires each Member State to adopt a national cybersecurity strategy and to establish or designate authorities responsible for cybersecurity and the management of large-scale cybersecurity incidents and crises.[176] Furthermore, Member States shall adopt laws to ensure that essential and important public and private entities take technical, operational and organizational measures to manage cybersecurity risks and minimize the impact of security incident on the recipients of their services.[177] Essential and important entities include, *inter alia*, public administration entities of the central government, providers of important digital infrastructures and certain large companies that are active in the healthcare, transport, or energy sector.[178] The NIS 2 Directive is complemented by sector-specific measures, including the European Electronic Communications Code (EECC)[179] and the Digital Operational Resilience Act (DORA)[180].[181]

48 Finally, the capacity of the EU and its Member States to fend off cyberattacks and related incidents shall be further strengthened by the Cyber Solidarity Act.[182] The Cyber Solidarity Act aims to strengthen European capacities to detect and respond to cybersecurity threats and incidents through the deployment of a pan-European infrastructure of Security Operation Centers to enhance detection capabilities (European Cyber Shield), the creation of a Cybersecurity Emergency Mechanism to support Member States in responding to and recovering from large-scale cybersecurity incidents, and the establishment of a review mechanism for large-scale incidents.[183]

IV. Strengthening Europe's Technological Independence

49 In addition to promoting its digital sovereignty, the EU is implementing legislation specifically aimed at advancing its technological and economic independence by increasing the availability of essential digital technologies, infrastructures, and data within Europe. These measures – although serving a conceptually different purpose – are closely related to the EU's pursuit of digital sovereignty, because an increase in Europe's technological independence and capabilities can also facilitate the EU's *de facto* control over its domestic cyberspace.[184] Key legislative measures to improve Europe's technological independence target the increased production of semiconductor chips in Europe (**1.**), the development and use of AI in Europe (**2.**), and the fostering of a competitive European data economy (**3.**).

1. Availability of Semiconductors

50 As semiconductors have become an essential input

172 Regulation (EU) 2019/881. For an account of the development of EU cybersecurity law see further Lee A. Bygrave, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes', (2025) 56 Computer Law & Security Review 106071.

173 Regulation (EU) 2024/2847. For an introduction to the Cyber Resilience Act see Pier Chiara, 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', (2022) 3 International Cybersecurity Law Review 255.

174 See Articles 5-9 and Recitals 6 and 7 of the Cybersecurity Regulation (Regulation (EU, Euratom) 2023/2841).

175 Directive (EU) 2022/2555.

176 See Articles 7-9 and Recitals 48-57 NIS 2 Directive.

177 See Article 21 and Recitals 77-89 NIS 2 Directive.

178 See Article 3 and Recitals 15-19, 31-35 NIS 2 Directive.

179 Directive (EU) 2018/1972.

180 Regulation (EU) 2022/2554.

181 Among other goals, the EECC shall ensure that providers of public electronic communications networks and services take appropriate technical and organizational measures to manage the (cyber) security risks posed to their networks and services; *see* Article 40 and Recitals 94-98 EECC. The objective of DORA is to achieve a high level of digital operational resilience in the financial sector; see Article 1(1) and Recital 12 DORA. Pursuant to Article 1(2) DORA and Article 4 NIS 2 Directive, the NIS 2 Directive does not apply to financial entities covered by DORA.

182 Regulation (EU) 2025/38..

183 See Article 1(1) and Recitals 7, 8, 13-15, 30, 35-38, and 50 of the Cyber Solidarity Act.

184 See infra Part D.II.

for the production of electronic goods[185], the EU Chips Act[186] presents an important building block in the EU's efforts to improve its technological independence. Its overarching goal is to provide "*a framework for increasing the Union's resilience in the field of semiconductor technologies*".[187] It primarily aims to do so by establishing the *Chips for Europe Initiative*, by improving the security and resilience of supply chains, and by supporting the government structures required for monitoring the semiconductor sector and responding rapidly to potential supply shortages.[188] In particular, the *Chips for Europe Initiative* will provide generous financial support to the establishment of factories for semiconductor production and related research in Europe.[189]

2. Leadership in AI

51 The EU intends to improve the AI capacities of European businesses and to promote the uptake of this new technology in Europe.[190] From a legal side, this goal shall be supported by the AI Act. In addition to mitigating the risks associated with AI, the AI Act aims to promote the development, use, and adoption of AI technologies in Europe by establishing harmonized rules for AI and improving the EU's internal market.[191] Furthermore, the AI Act provides for the establishment of regulatory sandboxes for the development, testing, and validation of innovative AI systems.[192] The purpose of regulatory sandboxes is to "*foster AI innovation by establishing a controlled experimentation and testing environment*" under the supervision of regulatory authorities.[193]

3. Data Economy

52 The EU is further determined to provide European businesses with better access to data as a key resource for innovation in order to reshape the competitive balance of the global data economy.[194] Consequently, the EU aims to increase the level of data sharing within the EU by amending the legal framework for data sharing through the DGA, the DA and the Common European Data Spaces.[195]

53 The DGA aims at facilitating the emergence of functioning data markets by promoting trust in so-called data intermediation services through the strict *ex ante* regulation of these services.[196] Besides improving the control of data subjects over their personal data[197], these regulated data intermediaries shall act as matchmakers on C2B and B2B data markets. In particular, they shall support data holders and data subjects in making their respective data available to potential data users, thereby increasing the availability of data for European businesses.[198] The DA is intended to improve data access for European businesses by removing certain barriers to data sharing which currently prevent an optimal allocation of data.[199] It does so by introducing access rights of product users and certain third parties to the data generated by the use of products connected to the internet.[200] These data access rights shall not only empower the users of connected products and achieve a fairer distribution of the benefits based on data generated by connected products.[201] They shall also unlock large amounts of data for innovation purposes of businesses and thus create significant economic welfare gains for the European economy.[202]

54 Finally, these two cross-sectoral legislative measures aimed at improving data availability are complemented by efforts to establish Common European Data Spaces in sectors of high importance, such as the health sector, the financial sector, or the agricultural sector.[203] This sector-specific approach reflects the need to take into account the individual circumstances of certain sectors and industries and

185 Monsees & Lambach (n. 18), 386.
186 Regulation (EU) 2023/1781.
187 Recital 2 of the Chips Act.
188 See Chapters 2-4 of the Chips Act. For a closer look see Dennis-Kenji Kipker, 'Technologie-Souveränität durch europäische Gesetzgebung? – Der Entwurf des neuen EU Chips Act und sein regulatorisches und politisches Framework', (2022) Kommunikation & Recht [K&R] 47.
189 See Articles 3(2) and 4(1) of the Chips Act.
190 European Commission, COM(2020) 65 final, 1. On the EU's approach to counter the legal and ethical risks associated with the use of AI see supra Part C.I.1.
191 See Recitals 1 and 8 AI Act.
192 See Articles 57-63 AI Act.
193 Recital 139 of the AI Act.
194 Pascal D. König, 'Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept', (2022) 8 European Policy Analysis 484, 497; Roberts et al. (n. 38), 9; von Ditfurth & Lienemann (n. 80), 272.
195 European Commission, COM(2020) 66 final, 12-14, 21-23.
196 See Recitals 5, 32 and Article 12 DGA; see also von Ditfurth & Lienemann (n. 80), 278.
197 See supra Part C.I.1.
198 Recital 27 DGA; European Commission, SWD(2020) 295 final, 1, 19-20; von Ditfurth & Lienemann (n. 80), 277.
199 See Recitals 2 and 4 DA.
200 On the data access rights under the DA see supra Part C.I.3.
201 See supra Part C.I.3.
202 See European Commission, Data Act Explanatory Memorandum, COM(2022) 68 final, 2-3; European Commission, SWD(2022) 45 final, 26-27, 40; Kerber, (n. 118), 122.
203 European Commission, COM(2020) 66 final, 21-23; European Commission, SWD(2022) 45 final, 1; European Commission, SWD(2024) 21 final, 17-38.

to assist them in developing tailor-made rules for data use and sharing.[204]

D. Evaluation

55 As the previous Section has shown, the EU has adopted extensive legislation in order to enhance its control over the digital space and to promote EU values and interests. However, while it is natural for the EU to seek to strengthen its control over cyberspace, the pursuit of digital sovereignty also raises questions about the overall desirability and appropriateness of the EU's approach to regulating cyberspace.

I. The Value of Digital Sovereignty

56 Digital sovereignty is inherently tied to the values of autonomy and the rule of law. The ability to shape the domestic law in a way that is not or only to a relatively limited extent controlled or influenced by foreign actors allows a state to pursue its objectives in a self-determined manner. And a state having the capabilities to effectively enforce its rules for the digital space ensures conformity with its domestic law, which is essential for securing whatever purposes the law is intended to serve.[205] At the same time, these virtues of digital sovereignty can also lend themselves to states' pursuit of immoral or imprudent purposes. Ultimately, the (moral) value of digital sovereignty thus depends on the goals that are being pursued through the exercise of sovereignty. Digital sovereignty can therefore be seen as a second-order goal, one that is pursued in order to further other first-order goals. The range of first-order goals for which digital sovereignty can be pursued is broad. A state's control over the digital space could be used to promote human rights or to maintain autocratic regimes and suppress dissent.[206] In this sense, digital sovereignty is morally neutral.

57 As seen in the previous Section, the EU's pursuit of digital sovereignty is primarily aimed at promoting human rights, democracy, and market fairness and competition as first-order goals. The promotion of these first-order goals is *prima facie* justified and desirable. Yet, whether the EU's pursuit of digital sovereignty will turn out to be successful ultimately depends on the suitability of its legislative measures for promoting these first-order goals. Conclusively answering this complex question would require an in-depth assessment of each legislative act related to the EU's quest for digital sovereignty, a task that cannot be accomplished here.[207] Instead, only some of the more general issues raised by the EU's quest for digital sovereignty will be discussed in this Section.

II. Lack of Coherence

58 The EU's pursuit of digital sovereignty, on the one hand, and of technological and economic independence, on the other hand, suffers from a lack of coherence. It is marred by a tension between the goals of protecting the rights of EU citizens and of promoting Europe's digital economy.

59 In theory, the two objectives of promoting European digital sovereignty and technological independence could complement each other. The existence of leading European technology companies and digital services providers could contribute to the effective enforcement of EU values and rules in cyberspace. For example, the emergence of high-quality European online services would mitigate current enforcement risks due to international data transfers.[208] Moreover, the emergence of European technologies can help spread and implement European values and interests in Europe and globally. European developers of AI systems could be more sensitive to European rights and values and infuse them into their systems. In the digital space, technological capabilities are not only vital for a region's economic competitiveness but also for its political power to shape the rules and

204 European Commission, COM(2020) 66 final, 6. As of today, the establishment of the European Health Data Space has progressed the furthest. Regulation (EU) 2025/327 on the European health data space has entered into force on March 26, 2025 and will start applying in 2029.

205 On this value of the rule of law see Joseph Raz, *The Authority of Law* (2nd edn, 2009) 223-226.

206 Pohle & Thiel (n. 11), 9-10; Chander & Sun (n. 27), 289, 293-298.

207 For example, the expected effects of the DMA are controversial. Some scholars support the DMA's goals and design, *see*, e.g., Cabral et al., *The EU Digital Markets Act: a Report from a Panel of Economic Experts* (2021) 30-32 <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122910/jrc122910_external_study_report_-_the_eu_digital_markets_acts.pdf>; Anne C. Witt, 'The Digital Markets Act: Regulating the Wild West', (2023) 60 Common Mkt. L. Rev. 625. Others are more skeptical, see, e.g., Carmelo Cennamo et al., 'Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act', (2023) 14 Journal of European Competition Law & Practice 44; Yunsieg P. Kim, 'A Revolution Without A Cause: The Digital Markets Act and Neo-Brandeisian Antitrust', (2023) Wis. L. Rev. 1247.

208 It is for this reason that Alexander Roßnagel, the Data Protection Commissioner of the German state of Hesse, claims that Article 8 of the Charter requires the EU and its Member States to promote the emergence of European digital services, see Roßnagel, (n. 24), 67.

values of cyberspace.[209]

60 Conversely, the exercise of sovereignty through digital regulation could also promote the technological and economic independence of Europe. The EU strategy for regulating data and digital markets not only pursues the protection of European values and rights, but also aims to advance Europe's economic interests.[210] In particular, the EU regulation of digital and data markets through the DMA, DGA, and DA can be seen as an attempt to promote the emergence of a competitive European data economy by reigning in the market power of dominant foreign competitors and reducing competitive disadvantages of European tech companies due to a lack of data availability.[211]

61 In practice, however, the two objectives seem to be at odds rather than complementing each other. It is likely that the EU's attempts to comprehensively regulate the digital economy weaken the European technology sector by limiting the use of new and innovative technologies and imposing high compliance costs on businesses. In particular, the GDPR, the centerpiece of European data regulation, likely has negative effects on innovation, competition, and economic welfare in the EU.[212] For instance, the GDPR's restrictions on collecting, retaining, and sharing data limit the availability of data necessary for training AI systems.[213] Furthermore, its strict principles of data minimization and purpose limitation work against the EU's objective of facilitating the broad use and sharing of data for business purposes through the DGA and DA.[214] This may lead to a pragmatic conflict between the GDPR and data sharing laws, as they promote diverging states of affairs that practically cannot coexist with each other.[215] Against this background, it is not surprising that European businesses regard the GDPR as the main obstacle to using and exchanging data for innovative purposes.[216]

62 In addition, the EU's recent approach of promoting digital technologies and services through rights-based regulation, which underlies both the AI Act and the DGA, is unlikely to succeed. The AI Act seeks to promote the development and uptake of AI in the EU by implementing harmonized rules for AI, which shall ensure a high level of protection of health, safety, and fundamental rights.[217] It is more likely, however, that its additional and often uncertain rules will further reduce the ability and willingness of European businesses to develop and use such technologies.[218] Similarly, the DGA is supposed to facilitate the emergence of data intermediation services by increasing trust in these services through strict regulation.[219] Yet, this approach is likely to backfire, as the strict and highly uncertain rules of the DGA will complicate the provision of data intermediation services and lead to high compliance costs.[220] In these instances, the EU's approach of promoting innovation through strict regulation is likely to end up harming rather than promoting Europe's innovative capabilities and technological independence.

209 Monsees & Lambach (n. 18), 380.

210 European Commission, COM(2020) 66 final, 1, 3; Bauer & Erixon (n. 13), 6.

211 König (n. 194), 497; Roberts et al. (n. 38), 9; von Ditfurth & Lienemann (n. 80), 272.

212 See, e.g., Michal S. Gal & Oshrit Aviv, 'The Competitive Effects of the GDPR', (2020) 16 Journal of Competition Law & Economics 349; Rebecca Janßen, 'GDPR and the Lost Generation of Innovative Apps', (2022) NBER Working Paper 30028 <https://www.nber.org/papers/w30028>.

213 Andrea Calderaro & Stella Blumenfelde, 'Artificial intelligence and EU security: the false promise of digital sovereignty', (2022) 31 European Security 415, 428; Erik Brattberg, Raluca Csernatoni & Venesa Rugova, 'Europe and AI: leading, lagging behind, or carving its own way?', (2020) Carnegie Endowment for International Peace Working Paper, 33 <https://carnegie-production-assets.s3.amazonaws.com/static/files/BrattbergCsernatoniRugova_-_Europe_AI.pdf>.

214 On this inherent tension in EU data law see generally Christiane Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (2017) 327. Neither the DGA nor the DA successfully address this tension, see Hennemann et al. (n. 117), 40-42.

215 On pragmatic conflict between laws see Raz (no. 205), 201.

216 See Jan Büchel et al., *Anreizsystem und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft* (2022) <https://ieds-projekt.de/wp-content/uploads/2022/03/IEDS-Whitepaper-1.pdf>; Bitkom, *After 5 years: GDPR only receives the grade "sufficient"* (Oct. 5, 2023) <https://www.bitkom.org/EN/List-and-detailpages/Press/5-years-GDPR-receives-grade-sufficient>.

217 See Article 1(1) and Recitals 8, 176 of the AI Act.

218 See, e.g., Bomhard & Merkle (n. 86), 283; Michael Veale & Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach', (2021) Computer und Recht international [Cri] 97, 112; Philipp Hacker, 'A legal framework for AI training data: from first principles to the Artificial Intelligence Act', (2021) 13 Law, Innovation and Technology 257, 298.

219 See Recitals 5, 32 DGA.

220 Richter (n. 80), 465; von Ditfurth & Lienemann (n. 80), 290.

III. Unilateralism

63 Traditionally, the EU has pursued a strategy of open markets and a multilateral approach to international diplomacy and this long-standing commitment is reflected in the EU Treaties.[221] According to Article 21(1) and (2)(h) TEU, the EU "*shall promote multilateral solutions to common problems*" and "*promote an international system based on stronger multilateral cooperation and good global governance*". The EU's pursuit of digital sovereignty is at odds with its multilateralist commitments, as it seeks to unilaterally regulate the digital space.[222] Due to the transnational nature of the digital space, this approach inevitably affects the autonomy (and thus the sovereignty) of other states. In particular, EU digital legislation can influence *de jure* or *de facto* rules in third states **(1.)**, contribute to the fragmentation of cyberspace **(2.)**, and promote economic protectionism **(3.)**.[223]

1. Extraterritorial Influence of EU Legislation

64 Some EU regulations, in particular the GDPR, the AI Act, the DGA, and the E-Evidence Regulation, share certain characteristics by which they influence the laws of foreign states and the behavior of foreign citizens and businesses.

65 The GDPR extends its geographic reach beyond the borders of the EU and directly covers certain online activities of individuals and businesses in third states.[224] Under its marketplace principle, the GDPR unilaterally extends the EU's legal authority over persons and organizations in third states.[225] In addition, the GDPR influences the laws of third states via its regulation of international data transfers. Personal data may only be transferred to a third country, if the EU Commission has decided that the third country ensures an adequate level of data protection or if the controller or processor transferring the data has provided appropriate safeguards to guarantee the effective protection of data.[226] The prospect of obtaining an adequacy decision from the EU Commission creates significant incentives for third states to align their data protection law with the GDPR.[227] For example, the pressure to satisfy EU adequacy requirements had an enormous influence on the emergence and shape of African data protection legislation.[228] These extraterritorial legal effects are reinforced by the Brussels Effect, which describes the unilateral extension of a state's laws beyond its borders through market mechanisms, leading to a *de facto* global reach of some EU rules.[229]

66 It is likely that other recent legal acts which include mechanisms similar to those of the GDPR will soon also exert their extraterritorial influence on foreign states. The GDPR's marketplace principle has been copied by the DSA, DGA, DA, and AI Act, extending their scopes to all relevant businesses operating in the EU's internal market, regardless of where these are established.[230] In addition, the DGA and DA mirror the GDPR's approach to regulating cross-border data flows data by restricting international transfers of non-personal data to third countries.[231]

67 Due to the borderless nature of the digital space, the implementation of legal mechanisms with extraterritorial effects can be necessary to effectively

221 Marise Cremona, 'Extending the Reach of EU Law: The EU as an International Legal Actor', in Marise Cremona & Joanne Scott (eds), *The EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019) 64, 66.

222 This is not surprising. Since the 20th century, the ideal of sovereignty has been frequently criticized for supposedly undermining multilateral cooperation and international law; see Philpott (n. 31), 568-571.

223 This Article will not delve into an analysis of the compatibility of the EU's regulation of cyberspace with international (trade) law. On this issue see Nehra Mishra, *International Trade Law and Data Governance* (2024); Roman Kalin, *Digital Trade and Data Privacy* (2024).

224 Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona & Joanne Scott (eds), *The EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019) 112; Koloßa (n. 147), 795; Federico Fabbrini & Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders', (2020) 21 Ger. Law J. 55, 61.

225 See supra Part C.II.2.; Azzi (n. 145), 130. This extension of the GDPR beyond EU borders raises problems under public international law, as it may conflict with the principles of legal sovereignty and non-interference, see Koloßa (n. 147), 798-807; Azzi (n. 145), 130-32.

226 Articles 44-49 GDPR; see supra Part C.II.1.(b).

227 Kuner (n. 224), 133; Mishra, (n. 223), 133.

228 Lukman Abdulrauf, 'African Approach(es) to Data Protection Law' in Raymond Atuguba, Moritz Hennemann, Patricia Boshe & Sena Afua Dei-Tutu (eds), *African Data Protection Laws* (2024) 36-39.

229 Anu Bradford, 'The Brussels Effect', (2012) 107 Nw. U. L. Rev. 1, 3; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (2020) 1-2. On the GDPR's tangible impact on Canada see René Mahieu et al., 'Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?', (2021) 11 Journal of Information Policy 301.

230 See supra Part C.II.2.x

231 See Article 31(1) DGA; Article 27(1) DA.

regulate domestic online activities.[232] For example, it would be easy to circumvent the high standard of data protection in the EU if personal data could be exported from Europe to third states without any conditions or restrictions.[233] Yet, the EU's approach goes beyond simply ensuring the effectiveness of its domestic regulations in a defensive manner and, in some instances, seeks to assert its values as universal values and to set global standards.[234] It was in this spirit that former EU Commissioner Viviane Reding advocated for the GDPR to become the "gold standard" for the world.[235] Similarly, the AI Act explicitly aims to shape global norms for AI.[236] Most notably, the E-Evidence Regulation disregards the territorial sovereignty of third states by requiring foreign service providers to hand over evidence data located on servers in third countries to European law enforcement agencies and by asserting the primacy of EU law in case of a conflict with foreign laws.[237]

68 Such offensive exercises of normative power can provoke conflicts with the interests and values of third countries.[238] It is hardly surprising then that foreign countries perceive the EU's *de jure* or *de facto* global regulation of cyberspace as attacks on their own digital sovereignty.[239] Therefore, the EU's extraterritorial regulation carries some risk of undermining multilateral cooperation and provoking sovereignty conflicts with third countries, if they decide to mirror the EU's approach.[240] Furthermore, it is possible that the extraterritorial imposition of EU legal values ignores important cultural and economic differences and is therefore ill-suited to address the needs and interests of some third countries.[241] The extraterritoriality of its legislation thus saddles the EU with a global responsibility that is difficult to fulfil.[242]

2. Fragmentation of Cyberspace

69 The EU's promotion of its digital sovereignty can also contribute to the fragmentation of cyberspace, thereby posing a threat to the global uniformity of the internet. According to Milton Mueller, digital sovereignty is "*inimical to [the internet's] liberalized order of information around common technical standards and the free flow of information*".[243] By disrupting global information flows as well as digital trade and services, national efforts to establish sovereign digital territories could divide the cyberspace. In this case, internet users around the world would no longer share the same online experience and this would have undesirable social, economic, and technical consequences.[244] For example, the restrictive regulation of online speech and content in some states may lead to the emergence of different cultural and social spheres on the internet.[245]

70 From an economic perspective, the proliferation of divergent national rules for digital technologies and online services increases compliance and transaction costs and jeopardizes global competition and free trade on the internet.[246] For instance, the emergence of a large number of divergent national adequacy standards for international data transfers has led to a fragmentation of data protection standards around the world, which especially harms businesses from the global south and small and medium-sized enterprises.[247] Ultimately, the divergent approaches to internet regulation may also affect the underlying hardware and networks themselves.[248] Fragmentation at the technical level could undermine the interoperability of hardware and disrupt the interconnectedness of the internet.[249]

232 See supra Part C.II.2.; Azzi (n. 145), 130.

233 Kuner (n. 139), 107.

234 Kuner (n. 224), 136; Glasze et al. (n. 1), 932; André Barrinha & G. Christou, 'Speaking sovereignty: the EU in the cyber domain', (2022) 31 European Security 356, 369.

235 See Viviane Reding, 'A data protection compact for Europe' (Jan. 28, 2014) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_62>. The European Commission has also articulated the GDPR's universal ambition in some of its official documents; see European Commission, COM(2017) 7 final, 2.

236 See European Commission, AI Act Explanatory Memorandum, COM(2021) 206 final, 5.

237 See supra Part C.II.1.(a).

238 On the EU's normative power see Ian Manners, 'Normative Power Europe: A Contradiction in Terms?', (2002) 40 Journal of Common Market Studies 235.

239 Celeste (n. 4), 224.

240 Kuner (n. 224), 138; Celeste (n. 4), 225.

241 See, e.g., Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets', (2021) 53 Vand. L. Rev. 685, 706; Anne Bernzen, "Data Colonialism?' Big Data's Adverse Impact on the (Global) South' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 171, 180-81; Payal Arora, 'General Data Protection Regulation – A Global Standard?: Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South', (2019) 17 Surveillance & Society 717, 718.

242 Kuner (n. 224), 142. See also Celeste (n. 4), 226; Matthias Braun & Patrik Hummel, 'Sovereign Power: Artificial Intelligence and Europe's Digital Sovereignty', (2023) 28 Geopolitics 932, 934.

243 Mueller (n. 9), 780.

244 Mark A. Lemley, 'The Splinternet', (2021) 70 Duke L.J. 1397, 1399.

245 Lemley, ibid, 1409.

246 Mueller (n. 9), 794.

247 Anupam Chander & Paul Schwartz, 'Privacy and/or Trade', (2023) 90 U. Chi. L. Rev. 49, 54, 107-8.

248 Lemley (n. 244), 1410-18.

249 See, e.g., on China's attempt to introduce its own technical standards Stacie Hoffmann et al., 'Standardising the

71 Not all of the EU's recent regulatory efforts necessarily contribute to the fragmentation of the internet.[250] To a certain extent, the internet can still function well if it is uniform in some respects and diverse in others.[251] This is illustrated by the EU's regulation of online speech. Although certain social media platforms operating in Europe, such as X (Twitter) or Facebook, have responsibilities under the DSA to moderate speech on their platforms in a manner that may be incompatible with the First Amendment, this has not led to a significant disruption of these platforms as transatlantic channels of communication.[252] However, from an economic perspective of free trade and competition, the EU's pursuit of digital sovereignty can be more problematic. Foreign businesses, especially SMEs, may find it difficult to navigate the complex web of the EU's digital regulatory environment and could be kept from entering the European market due to pre-emptive compliance costs. The stringent regulation of novel technologies in the EU, such as AI, can also lead to a divergence in the types of services and applications offered to users inside and outside the EU.[253] In some instances, this can deprive Europeans of access to innovative technologies and services.[254]

3. Economic Protectionism

72 Partly due to their fragmenting impact, many of the EU's digital policies and legislative acts have been accused of protectionist rationales.[255] Critics regard the EU's pursuit of digital sovereignty and technological independence as a pretext for a hidden protectionist agenda.[256]

73 In the US, it is particularly the EU's regulation of large online platforms through the DMA that is perceived as a protectionist attack on its largest and most successful Internet companies, as five of the seven designated gatekeepers covered by the DMA are American (Alphabet, Amazon, Apple, Meta, and Microsoft).[257] Another frequent target of anti-protectionist criticisms are the EU rules on international transfers of data.[258] These are regarded by some as "data localization" measures, i.e., measures that specifically restrict cross-border data transfers.[259] Critics of such measures argue that these measures are often motivated (at least implicitly) by the aim to promote domestic economic development, but instead end up harming domestic and foreign businesses and consumers by raising costs, limiting access to foreign services, and impeding technological progress.[260]

74 It is hard to determine to what extent these accusations are justified. As Christoph Kuner has

splinternet: how China's technical standards could fragment the internet', (2020) 5 Journal of Cyber Policy 239, 252-254.

250 Lemley (n. 244), 1401.

251 Woods (n. 52), 368.

252 See also Nick Clegg, 'The Future of Speech Online: International Cooperation for a Free & Open Internet', (2024) 153 Daedalus 65, 70.

253 European Parliament Research Service, *'Splinternets': Addressing the renewed debate on internet fragmentation* (2022) 42 <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf>.

254 For example, Apple delayed the EU release of the iPhone 16's AI feature for 18 months due to concerns over its compliance with the DMA; see Dwayne Cubbins, 'Apple Intelligence in Europe: What's happening and why the hold-up?', Tech-Issues Today (Sep 10, 2023) <https://techissuestoday.com/apple-intelligence-europe-availability>. This shows that not every EU regulatory act will necessarily lead to the Brussels Effect. In cases where the provision of services can be split between different territories at a reasonable cost, businesses will not need to comply with EU laws extraterritorially.

255 Pohle & Thiel (n. 11), 11; Dennis Broeders et al., 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions', (2023) Journal of Common Market Studies 1, 8; Chander & Sun (n. 27), 310.

256 See, e.g., Charlene Barshefsky, 'EU digital protectionism risks damaging ties with the US', Financial Times (Aug. 2, 2020) <https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103>.

257 For example, a bipartisan group of members of Congress sent a letter to then President Biden stating that "*as European leaders have made clear, the DMA as currently drafted is driven not by concerns regarding appropriate market share, but by a desire to restrict American companies' access to Europe in order to prop up European companies*" <https://delbene.house.gov/uploadedfiles/eu_digital_markets_act_letter.pdf>; see further EU Commission, *Digital Markets Act: Commission designates six gatekeepers* (Sep. 6, 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328>.

258 Susan A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', (2019) 18 World Trade Review 541, 557-562; Henry Farrell & Abraham Newman, 'The Transatlantic Data War', Foreign Affairs (Feb. 2016) <https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war>.

259 Anupam Chander & Uyên P. Lê, 'Data Nationalism', (2015) 64 Emory L. J. 677, 680; Naef, (n. 141), 235. Due to these restrictive effects, the regulation of international data flows under the GDPR has raised doubts about its compatibility with the non-discrimination obligations of the WTO's General Agreement on Trade in Services (GATS); see, e.g., Svetlana Yakovleva & Kristina Irion, 'Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation', 114 AJIL Unbound, 10 (2020); Mira Burri, 'Interfacing Privacy and Trade', (2021) 53 Case W. Res. J. Int'l L. 35, 62-67.

260 Chander & Lê, ibid, 721; Martina F. Ferracane, 'The Costs of Data Protectionism' in Mira Burri (ed), *Big Data and Global Trade Law* (2021) 69.

pointed out, it is often difficult to accurately identify protectionist policy rationales and distinguish them from other underlying motivations.[261] Because of cultural differences in their views on the nature and value of data protection, strict data protection laws may appear legally and morally justified to a European and protectionist to an American.[262] This observation also applies to other areas of digital regulation that are central to the EU's quest for digital sovereignty, such as the regulation of online speech, AI, and competition in digital markets. In defense of the EU, it can be argued that both the DMA and the regulation of international data transfers pursue rational and legitimate aims. The DMA's objectives of strengthening the contestability and fairness of markets for core platform services are based on justified economic concerns and do not arbitrarily disadvantage foreign companies. Similarly, the GDPR aims to prevent circumventions of EU law and to guard against concrete risks for personal data in other countries, such as broad data access rights for law enforcement authorities or intelligence agencies.[263] Still, it cannot be ruled out that these laws may have *de facto* protectionist effects.

75 More problematic than these value-based regulations are the EU's efforts to strengthen its technological independence, which carry overt protectionist connotations.[264] After all, the objective of technological independence is driven by the desire to substitute foreign technology providers with local ones and to increase the market shares of domestic tech companies. In some cases, there are plausible policy reasons for strengthening the technological and digital capabilities of European companies. Heavy reliance on foreign technology providers can sometimes undermine Europe's cybersecurity and its autonomy.[265] However, there is a fine line between policies based on such legitimate reasons and policies whose protectionist effects are not justified by adequate policy rationales.[266] The mere fact that certain technologies or services are developed abroad should not serve as a blanket excuse for the preferential treatment of local providers.

261 Christopher Kuner, 'Data Nationalism and its Discontents', (2015) 64 Emory L.J. Online 2089, 2097.

262 For an overview of the different visions of data privacy in the EU and the US see Paul M. Schwartz & Karl-Nikolaus Pfeifer, 'Transatlantic Data Privacy Law', (2017) 106 Geo. L.J. 117, 121-137.

263 Kuner (n. 261), 2093; Kuner (n. 139), 107-116.

264 Bauer & Erixon (n. 13), 22.

265 Theodore Christakis, *European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy* (2020) 54-55 <https://ssrn.com/abstract=3748098>.

266 Christakis, ibid, 54.

E. Conclusion

76 Ultimately, it is easy to see why the ideal of a digitally sovereign EU has such a broad appeal. At a time when many undesirable social, economic, and political effects of the internet have become apparent, the EU understandably feels the need to actively and self-determinedly shape and enforce the rules governing cyberspace on its own digital territory. By embracing digital sovereignty as a normative ideal, the EU's digital agenda has shifted towards prioritizing control over its domestic cyberspace.[267] Digital sovereignty serves as the overarching goal that connects different pieces of legislation, all of which share the aim of redefining the prevailing rules of the digital space and restoring the EU's control over its digital territory. By implementing rules to protect the rights of individual citizens, the functioning of democracy and competition in digital markets, the EU is pursuing a regulatory path that sets itself apart from both the market-centric approach of the US and the state-centric approach exemplified by China.[268]

77 It is likely that the EU will continue to focus on its digital sovereignty during the second term of von der Leyen's commission presidency. This is indicated by the fact that the European Commission has for the first time appointed a Vice-President for Tech Sovereignty, Security and Democracy, whose goals include developing a Digital Fairness Act and promoting EU digital norms and standards internationally.[269] In general, this approach deserves support. As sovereigns, the EU and its Member States have the legal right and the legitimacy to set the rules governing Europe's digital space and the values pursued by the EU deserve protection.[270] Moreover, since the second Trump administration took office in the US, the need to continue to assert EU values and interests in cyberspace has only grown.

78 However, there are also inherent risks to openly embracing a legal policy centered on the pursuit of digital sovereignty. First, it can lead to false expectations and regulatory hubris. Digital regulation is characterized by a high degree of informational

267 See also Falkner et al. (n. 66), 2112.

268 See further Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (2023).

269 European Parliament Research Service, *Briefing: Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy* (2024) 3 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762455/EPRS_BRI(2024)762455_EN.pdf>.

270 Contrary to the ideology of early cyber-exceptionalists, states have remained the "*single greatest source of legitimate rules for different peoples with varied community values and experiences on a diverse planet*", *see* Woods (n. 52), 369.

uncertainty.[271] The difficulty of regulating a rapidly evolving technological environment with significant uncertainty about future developments and disruptions can lead to regulatory lag, off-target regulation, and other unintended consequences. Examples include the slow reaction of regulators to strategic acquisitions of emerging start-up competitors by big tech companies[272], the GDPR's long-winded legislative process and its failure to take into account looming big data and AI trends[273], and the neglect of general purpose AI, such as ChatGPT, in the European Commission's original Proposal for the AI Act.[274] Thus, the ideal of digital sovereignty may create expectations of a level of control over the digital space that is illusory and there is a risk that it may lead EU regulators to overestimate the accuracy and effectiveness of new potential legislation. In addition, the EU's control over the digital space can be constrained by its limited foreign policy competences, which may impair the EU's ability to strengthen its external digital sovereignty against interference by hostile states[275], and by the decentralized enforcement of EU law, which has often not been sufficiently effective, especially in cross-border contexts.[276]

79 Second, the embrace of digital sovereignty as a legislative ideal sits uneasily with the EU's traditionally multilateral and trade-friendly approach to international politics. More than most other areas of domestic policy, the regulation of the inherently transnational cyberspace can have direct legal, economic, and political effects on foreign states and their citizens.[277] Some of these effects may be unwelcome. Unilaterally pursuing EU values and interests through extraterritorial legislation may lead third countries to reciprocate[278], which would further fragment the rules of cyberspace. Already, the proliferation of laws with extraterritorial effects from different jurisdictions creates legal conflicts and dilemmas for the legal subjects who must choose whether to comply with the laws of one jurisdiction or another. For example, organizations may face incompatible legal obligations when confronted with data access requests under the US CLOUD Act on the one hand, and GDPR obligations not to disclose the data on the other.[279] A similar dilemma may arise soon as a result of the conflict between the E-Evidence Regulation and the US ECPA.[280]

80 As these examples also show, the EU exercises its digital sovereignty for both defensive and offensive purposes. In the first example, it is the US CLOUD Act that that challenges the EU's sovereignty and that is legitimately countered by the GDPR's defensive mechanisms for controlling data exports in order to protect the rights of EU data subjects. In contrast, the E-Evidence Regulation follows a more offensive approach. The EU intends to abandon the traditional concept of territoriality, which is tied to the location of the data, for its own data access requests, while still preserving its territorial sovereignty against foreign data access requests.[281] Such offensive exercises of digital sovereignty by the EU can understandably be perceived by foreign states as threats to their own digital sovereignty.

81 For these reasons, the EU should take a measured approach towards promoting its digital sovereignty, rather than pursuing digital sovereignty unconditionally and for its own sake. This requires the EU to critically assess the domestic and

271 Urs Gasser & Moritz Hennemann, 'Unlocking the Potential of the Data Age: Key Tasks and Challenges of Data Strategies' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 11, 15.

272 See Christophe Carugati, 'Which mergers should the European Commission review under the Digital Markets Act?', (2022) Bruegel Policy Contribution 24/2022, 2 <https://www.bruegel.org/system/files/2022-12/PC%2024%202022.pdf>.

273 See Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', (2017) 47 Seton Hall L. Rev. 995.

274 See the adopted position of the Council of the EU from Nov. 25, 2022, 2021/0106(COD), 6 <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

275 On the EU's disjointed approach to combating state-sponsored disinformation see Andreu Casero-Ripollés et al., 'The European approach to online disinformation: geopolitical and regulatory dissonance', (2023) 10 Humanities and Social Sciences Communications 657, 7; Matthias Kachelmann & Wulf Reiners, 'The European Union's Governance Approach to Tackling Disinformation: Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty', (2023) 396 L'Europe en formation 11, 17-21.

276 See, e.g., on the issues surrounding the GDPR's cross-border enforcement Giulia Gentila & Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR', (2022) 71 International & Comparative Law Quarterly 799. As a result, the EU Commission is seeking to improve the GDPR's cross-border mechanisms, see Chapter III of its Proposal for a Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final.

277 Chander & Sun (n. 27), 307; Moritz Hennemann, 'Global Data Strategies: An Introduction' in Moritz Hennemann (ed), *Global Data Strategies: A Handbook* (2023) 1, 1.

278 Kuner (n. 224), 138.

279 See Jessica Shurson, 'Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law', (2020) 28 International Journal of Law and Information Technology 167, 179-80.

280 See supra Part C.II.1.(a).

281 Suzan Hüttemann, 'Die E-Evidence-Verordnung: Pioniermodell für das digitale Zeitalter oder Preisgabe der Staatlichkeit?', (2024) Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht [NZWiSt] 81, 92.

international implications of existing and new legislation in order to ensure that it coherently and appropriately regulates the domestic cyberspace and avoids international legal conflicts.[282] Domestically, the EU will need to better align its goals of digital sovereignty and technological independence, as the current regulatory framework for digital technologies is likely to stifle innovation, development, and use of new technologies within the EU. Internationally, the EU should continue to avoid unilateral solutions where this is possible and seek multilateral cooperation among like-minded states.[283] In theory, a multilateral approach enables the EU to protect important values and interests while simultaneously respecting the sovereignty of third countries.[284]

82 Of course, a multilateral approach is only feasible if third states are willing to cooperate and compromise. Given the current tense international political climate and the diverging values and interests of some other major international powers, multilateral efforts alone are unlikely to effectively protect and promote EU values and interests in the digital space. In particular, the EU faces external pressures from the US and China, which are each advancing their own competing visions for regulating cyberspace.

83 China exports its illiberal and state-centric model for regulating the digital space through the provision of its homegrown digital infrastructures abroad and through its growing influence on international institutions, such as the United Nations or the International Electronical Commission (IEC).[285] The US model for governing the digital space, which is based on weak digital regulation and strong protections for free speech, is exported primarily through the commercial success of US tech companies.[286] During the second Trump administration, this laissez-faire approach towards digital regulation is likely to be more actively promoted by the US government, including in relation to the EU.[287] Already, members of the Trump administration have voiced harsh criticism of the EU's regulation of speech and AI.[288] There are also concerns that the Trump administration's actions could target the enforcement of the DMA[289] or unravel the EU-US Data Privacy Framework, putting data transfers from the EU to the US at risk.[290]

84 Where multilateral cooperation is thus unrealistic and there is a need to safeguard the EU's autonomy against external pressures, the pursuit of digital sovereignty for defensive purposes is necessary and legitimate to effectively protect European interests and values in accordance with Article 3(5) TEU.

282 Currently, impact assessments and evaluations of EU legislation are limited to domestic effects and do not take into account potential consequences for third countries; see Kuner (n. 224), 142.

283 Examples of this approach include the agreements on cross-border data transfers with Japan and the US and the recently concluded digital trade agreement with South Korea.

284 See also Woods (n. 52), 368-69. In some instances, the promotion of digital sovereignty may strengthen the EU's bargaining position, allowing it to gain more concessions from third countries.

285 See further Bradford (n. 268), 290-308, 388-93; Erie & Thomas Streinz, 'The Bejing Effect: China's Digital Silk Road As Transnational Data Governance', (2021) 54 N.Y.U. J. Int'l L. & Pol. 1, 35-47; Willem Gravett, 'Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa,' (2020) 20 Afr. Hum. Rts. L.J. 125, 138-42.

286 Bradford (n. 268), 33-52, 259.

287 See Jan Philipp Albrecht, 'Trump and Big Tech: Europe's Sovereignty at Stake', Heinrich Böll Stiftung (Jan 24, 2025) <https://www.boell.de/en/2025/01/24/trump-and-big-tech-europes-sovereignty-stake>.

288 See, e.g., Emily Atkinson, 'JD Vance attacks Europe over free speech and migration", BBC News (Feb 15, 2025) <https://www.bbc.com/news/articles/ceve3wl21x1o>; Clea Caulcutt, 'JD Vance warns Europe to go easy on tech regulation in major AI speech, Politico (Feb 11, 2025) <https://www.politico.eu/article/vp-jd-vance-calls-europe-row-back-tech-regulation-ai-action-summit/>.

289 See Stefan Krempl, 'Suspension of the DMA? – Concerns about horse-trading between the EU and the USA (Jun 26, 2025) <https://www.heise.de/en/news/Suspension-of-the-DMA-Concerns-about-horse-trading-between-the-EU-and-the-USA-10461509.html>

290 See Brian Hengesbaugh & Lukas Feiler, 'How could Trump administration actions affect the EU-US Data Privacy Framework?', IAPP (Feb. 26, 2025) <https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework>.