Digital Society (2022) 1:20
https://doi.org/10.1007/s44206-022-00021-3

COMMENTARY

The Politics of Data in EU Law: Will It Succeed?

Ugo Pagallo[1]

Received: 11 May 2022 / Accepted: 7 September 2022 / Published online: 21 September 2022

Abstract
The paper examines recent initiatives of the European Commission that aim to complement today's legislation on the internet, data governance, and technological innovation, and how scholars have attempted to sum up current trends of EU law according to some catchy formulas: digital sovereignty, digital constitutionalism, or a renewed Brussels effect. Although such narratives have their merits, they can also be misleading and should be taken with a pinch of salt. The paper intends to complement such narratives in connection with the open issues on the balance of powers between EU institutions and member states (MS), with a new generation of digital rights at both EU and MS constitutional levels, down to the interplay between new models of legal governance and the potential fragmentation of the system. Whether and to what extent EU law will be successful in the regulation of data-driven societies and complex digital ecosystems do not only regard acts, policies, and proposals against misuses and overuses of technology but also how well mechanisms of coordination and models of cooperation set up by EU law will fare against technological underuses with their opportunity costs.

Keywords Brussels effect · Data politics · Digital constitutionalism · Digital sovereignty · European Union (EU) law · Legal governance · Opportunity costs

1 Introduction

Scholars have increasingly stressed the dependency of human societies on information communication technologies (ICTs), and further emerging technologies such as artificial intelligence (AI) and robotics on the internet of everything (Floridi, 2014; Pagallo, 2015). Although human societies have been related to the use of ICTs over the centuries, they have been mainly dependent on technologies that regard energy and basic resources. What is new with today's societies concerns the fact that they progressively depend on ICTs and, furthermore, on information and data as a vital

✉ Ugo Pagallo
ugo.pagallo@unito.it

[1] University of Turin, Turin, Italy

resource. This data-driven scenario affects the understanding about ourselves and our world, raising a full array of normative challenges. The list of initiatives and acts presented by the European Commission, aiming to complement EU legislation on data protection, cybersecurity, digital economy, and technological data-driven innovation, illustrates the point. Table 1 sums up the legal sources more frequently mentioned in this paper, to properly set its level of abstraction, namely, the stance through which the paper intends to describe, examine, and argue about the politics of data in EU law.

The list of Table 1 does not aim to be exhaustive, but good enough to start addressing the intricacy of today's EU legal framework with its normative acts, policies, and proposals. The formula 'politics of data' adopted in the paper refers to this legal framework, considering the novelty of current human data-driven societies in accordance with a basic tenet of Aristotle's 'politics,' or 'practical sciences.' How shall the law strike the balance among multiple regulatory systems that compete in society, such as ethics and social mores, the forces of the market, and generally, what Aristotle dubs as "economics" in the eighth book of the *Nicomachean Ethics* (Aristotle, 2000)?

While, to the Aristotelian list, we must add affordances and restraints of technology as a regulatory system of its own, it is noteworthy that acts and proposals of EU data law concern all facets of Aristotle's politics: the ethical principles on trustworthy AI endorsed by the AIA, engagement of stakeholders (DGA, EU DS, ODF, etc.), the troubles with business and the market (DMA, DSA, DAct, etc.), and the development of new legal and technological standards (AIA, Cyber Act, EHDS, etc.). How all these acts, policies, and proposals of EU law strike the balance among multiple competitive regulatory systems has been the subject of an intense debate since the late 2010s. This paper will mostly deal with three narratives. The first one presents

Table 1 The sources of data politics in EU law

Acronym	Year	Source	Subject
AIA	2021	COM/2021/206 final	Artificial intelligence
CEAP	2020	COM/2020/98 final	Circular economy
Chips Act	2022	COM/2022/46 final	Semiconductors
Cyber Act	2019	Regulation 2019/881	Cybersecurity
DAct	2022	COM/2022/68 final	Fair data access and use
DGA	2020	COM/2020/767 final	Data governance
DHC	2018	COM/2018/233 final	e-Health and care
DMA	2020	COM/2020/842 final	Digital markets
DSA	2020	COM/2020/825 final	Digital services
ECL	2021	Regulation (EU) 2021/1119	Climate
EHDS	2022	COM/2022/197 final	Health data space
EU DS	2020	COM/2020/66 final	Overall data strategy
GDPR	2016	Regulation 2016/679	Personal data
Green Deal	2019	COM/2019/640 final	Climate, environment
ODF	2019	Directive 2019/1024	Open data framework

recent initiatives of the European Commission and new provisions of EU law as a "fight for digital sovereignty" (Couture & Toupin, 2019; Roberts et al., 2021): control over data, much as over software, standards, services, infrastructures, etc., is a crucial issue of power and geopolitics in current data-driven societies. A second stance refers to EU attempts to oppose the power of transnational corporations operating in cyberspace with both a new set of rights for individuals and obligations for such corporations. The fight for digital sovereignty could also be understood as an evolution of EU law towards "digital constitutionalism" (De Gregorio, 2020). Third, recent initiatives of the European Commission on AI, data governance, digital services or markets, etc., can be grasped with "the Brussels effect" (Bradford, 2012, 2020). The idea is that the non-divisibility of data and compliance costs of multinational corporations that deal with multiple regulatory regimes may prompt most technological manufacturers and service providers to adopt and adapt themselves to the strictest international standards across the board, that is, in many cases, just EU law (Pagallo, 2013).

Each of these narratives on digital sovereignty, digital constitutionalism, or the Brussels effect has the merit to draw our attention to critical aspects of today's data politics. They all cast light on crucial issues of power, rights, and interplay between multiple regulatory regimes and jurisdictions. However, they also should be taken with caution. Current discussions on sovereignty, new rights, and the impact of EU law on the rest of the world must be complemented with the analysis of further facets of the politics of data, such as risks of legal fragmentation and the role that mechanisms of coordination and methods of cooperation play in EU law.

To put things in perspective, the analysis of this paper is accordingly divided into three parts. The next section illustrates the merits and limits of today's debate on digital sovereignty, digital constitutionalism, and a new Brussels effect. Section 3 scrutinizes the limits of such catchy formulas with the further analysis on the balance of power between EU institutions and member states (MS), a new generation of digital rights at both EU and MS constitutional levels, down to new models of legal governance that shall address the challenges of current data-driven societies. Section 4 sums up the results of the analysis to finally answer in the conclusion, the question posed by the title of this paper: "will EU law succeed"?

Drawing on work in legal theory and governance models for the regulation of technology, the analysis rests on a twofold distinction. In light of the list of legal sources in Table 1, we should distinguish on the one hand between acts, policies, and proposals of EU law that hinge on the commands of legislators supported by the threat of physical or pecuniary sanctions (Sect. 2 of this paper), and on the other hand acts, policies, and proposals of EU law that revolve around mechanisms of coordination and cooperation (Sect. 3). This distinction between hard law and soft law, between top-down regulation and manifold forms of co-regulation will be finetuned, by distinguishing between acts, policies, and proposals of EU law against overuses and misuses of technology, and acts, policies, and proposals of EU law against underuses of technology and its opportunity costs (Sects. 3.2 and 3.3). The intent of this twofold differentiation between hard law and soft law, between misuses, overuses, or underuses of technology with their models of governance is to properly address the necessary temporary limits of the research, especially considering the on-going process of discussion, revision, and amendment of EU law proposals (Sect. 4). Whether and to

what extent EU data policies will be successful over the next months and even years — in enforcing its new top-down laws, preventing risks of technological obsolescence, or exerting extraterritorial effects over the market and other jurisdictions — remains an open issue. Still, it should be carefully distinguished from the further set of legal issues regarding the success of EU efforts in coordination and cooperation. This part of the EU's digital strategy appears as critical as the regulatory top-down efforts of EU legislators under scrutiny in the next section of this paper. We shall not overlook it.

2 On EU Hard Law and Its Limits

Hard law is an essential component of today's EU data politics. Current debates on digital sovereignty, digital constitutionalism, or a renewed Brussels effect have the merit to stress this hard side of the law, according to which the commands of lawmakers are supported by the threat of physical or pecuniary sanctions. Power and control over data (digital sovereignty), new rights (digital constitutionalism), and extra-territorial impact of legislations (the Brussels effect) will be examined in accordance with some of the acts, policies, and proposals introduced above with Table 1, and against the backdrop of EU treaties and principles. The aim of this section is twofold. On the one hand, the intent is to illustrate a new generation of binding provisions for the governance and regulation of data and data-driven technologies in EU law; on the other hand, the purpose is to stress that which narratives on digital sovereignty, digital constitutionalism, or the Brussels effect tend to overlook. Such legal issues either fall outside the power of EU institutions, e.g., public order and national security, or have recommended the adoption of further models of legal governance for technological innovation. This viewpoint on the limits of current debates on sovereigns, digital constitutionalism, and extra-territorial effects of EU legislation should put the hard law provisions of acts, policies, and proposals of EU law under a more proper light and perspective.

2.1 Digital Subsidiarity

Several communications on the digital strategy of the European Commission, the Parliament, or the Council present their strategy under the formula of 'digital sovereignty' (Arner et al., 2022; Roberts et al., 2021). The new informational dimension of an old concept, that is, "digital sovereignty" aims to draw the attention to the current fight for control over data and information among multiple regulatory systems in competition out there: the legal powers of national governments and international organizations; the forces of the market, and of social norms; the role of civic institutions and the financial sector, the constraints of technology, and more. Control over data and information regards EU initiatives in cloud computing and AI, the internet of things (IoT) and cybersecurity, mobile telecommunications, and supercomputing (Timmers, 2022). Although these fields raise critical challenges for both the EU and its MS, the overall idea to sum up the relevance

of such challenges in terms of digital sovereignty appears at least inappropriate, especially in the case of the communication services of the EU institutions.

From a strict legal viewpoint, there is indeed no place for any sovereign within EU law. For better or for worse, 30 years ago, the compromise on who must have the "last word" between EU institutions and MS was struck with the principle of subsidiarity pursuant to Art. 5 of the Maastricht Treaty from 1992. Several regulatory initiatives and proposals of the Commission, mentioned above in the introduction, rest on this principle. The complex legal framework summed up with Table 1 reminds us of that which triggers more often subsidiarity, i.e., the scale or dimension of the issues that are at stake with the digital strategy of the EU institutions: social interaction on the internet, data governance, or the normative challenges of AI and other emerging technologies. Such issues cannot be addressed but at the EU level. Subsidiarity covers the GDPR (recital 170): the AIA, the Chips Act, the DAct, or the EHDS (no. 2 of the corresponding explanatory memorandum).

Still, the reason why we should avoid any legal reference to the formula of "digital sovereignty" or at least we should use it with extreme care is not simply formal. The formula can be misleading to sum up current initiatives or acts of EU law for three further reasons. Digital sovereignty, first of all, may suggest that EU regulations look like federal law, but they are not. Transferred by MS and their constitutional powers through the Treaties, EU powers are not "original" as occurs with the constitutional powers of federal states, e.g., the United States (US). The second reason regards the balance of powers and necessary coordination between EU institutions and MS, as well as new models of governance on which recent proposals and initiatives of the Commission hinge. The notion of digital sovereignty echoes mechanisms of centralization, thus missing alternative approaches of governance, collaboration, and alliances in such sectors as cybersecurity and IoT, mobile telecommunications, and quantum technologies, that will be examined in the next section of this paper (Arner et al., 2022). The third reason concerns how we interpret attempts to oppose the powers of transnational corporations operating in cyberspace with a new set of responsibilities and duties for such corporations, either as providers of services on the internet, or as designers and manufacturers of high-risk AI systems, or as personal data controllers in complex digital environments. According to advocates of digital sovereignty (Madiega, 2020), the EU would have flexed its muscles, showing who is the digital sovereign today, by establishing new duties for the corporations of Silicon Valley, and new rights for the EU citizens. Starting with the right to delisting set up by the Court of Luxembourg in the Google case from 2014, there is a long list of new rights and initiatives that illustrates this trend: the rights to erasure, to be forgotten, to data portability, etc., enshrined in the GDPR; the rights not to be profiled, nor recognized by AI systems, proposed by Art. 5 of the AIA; the rights to access and use of data and right to share with third parties such data set up with Art. 4 and 5 of the DAct; the rights on the primary use of people's e-health data pursuant to Art. 3 of the EHDS; down to EU policies on open access rights, open science rights, etc. Over the past years, this new set of rights and proposals has increasingly been summed up as the "digital constitutionalism" of the

EU institutions (De Gregorio, 2020). Would this stance on rights and constitutions, rather than power and sovereigns, cast a more fruitful light on current trends of EU law?

2.2 Digital Rights and Duties

Advocates of digital constitutionalism, as much as the overlapping view of digital sovereignty, draw the attention to a distinct feature of EU law. Over the past 25 years and more, EU law has attempted to complement the traditional framework of basic constitutional (and human) rights associated with the physical body of the individuals and their *habeas corpus*, with a new principle of *habeas data*. The latter can be traced back to that which the German Constitutional Court has framed in terms of "informational self-determination" since its *Volkszählungs-Urteil* ('census decision'), from 1983. This principle of informational self-determination has often revolved in EU law around principles and safeguards of personal data protection. Recent proposals such as the AIA, the DAct, and the EHDS aim to complement this level of protection with further data rights and corresponding duties and obligations for e.g., gatekeepers of data-driven societies.

Against this framework, some claim that "in the last twenty years, the policy of the European Union in the field of digital technologies has shifted from a liberal economic perspective to a constitution-oriented approach" (De Gregorio, 2020). According to this perspective, drawing on the work of Waldron (2012) and Sajó and Uitz (2017), "the mission of modern constitutionalism is to protect fundamental rights while limiting the emergence of powers outside any control" (de Gregorio, 2020, at 3). In this respect, the amount of acts or proposals of the EU institutions is impressive: after the penalties set up with Art. 84 in the GDPR; the list of new duties and obligations includes the due diligence obligations for a transparent and safe online environment pursuant to Chapter III, Art. 10 ff. of the DSA; obligations of gatekeepers set up with Art. 5 and 6 of the DMA; the prohibitions, duties, and obligations for providers of AI high-risk systems established with the AIA; the obligations of manufacturers, importers, or distributors of e-health records systems, in accordance with Art. 17 ff. of the EHDS; down to new obligations for some data holders to make their data available pursuant to Art. 8 of the DAct.

This sort of EU digital constitutionalism, however, has its limits. All in all, the EU lacks the core of traditional constitutionalism, that is, power over matters of public order, law enforcement, and national security in such crucial fields as criminal and administrative law (including procedural safeguards). By referring to the formula of EU digital constitutionalism, the risk is to overlook the black hole in such framework, namely, rights and safeguards for the digital body of individuals vis-à-vis law enforcement officers, public prosecutors, or secret services. To understand how technology impacts certain tenets of the rule of law, such as the principle of habeas corpus and notions of "fair trial," of "equality of arms," etc., in the digital era (Pagallo & Quattrocolo, 2018), EU experts deal with the sovereign powers of their own state over criminal matters, security, and intelligence, although within the general framework provided by the 1950 European Convention of Human Rights

and its Court's (ECtHR) case-law, and the provisions of EU law. The limits of EU law vis-à-vis the sovereign powers of MS do not mean that EU law plays no role in criminal law (Mitsilegas, 2022), rather, that EU law and current acts and proposals for the regulation and governance of today's data-driven societies cover only a part, although important of the data rights of groups and individuals. Lest we start re-amending treaties and the charter of fundamental rights, we should not ask EU law for more than it can do in reasonable times. The full array of acts, policies, and proposals of EU law that shape its digital strategy should not overlook the role that MS and other jurisdictions, e.g., ECtHR case-law, play for the protection of new digital rights of groups and individuals. We return to this essential role of MS and the case-law of the courts below in Sect. 3.3.

2.3 Binding Rules and Digital Effects

The previous section mentioned some acts and proposals of EU law, such as the AIA, the DAct, the DMA, the DSA, the EHDS, or the GDPR that critically revolve around the top-down commands of lawmakers. As samples of hard law, such commands aim to govern individual and collective behaviour hinging on the threat of physical or pecuniary sanctions. By drawing the attention to the binding rules of EU law, debates on digital sovereignty and digital constitutionalism thus suggest the further question on whether such rules will be or are already effective. There are three different ways in which we can grasp such a question on the "effects of the law." First, the question may regard whether acts and proposals of EU law will be successfully enforced in the internal digital market. Second, we may wonder on whether EU law will be adopted or imposed in other jurisdictions, according to the stance that has become viral with Anu Bradford's formula on "the Brussels effect," that is, the power that EU law exerts beyond its own boundaries and jurisdiction in such fields as data protection, environmental law, or antitrust (Bradford, 2012, 2020). Third, the focus can be on whether such acts and proposals of EU law have been properly designed to attain their ends. It seems fair to admit that the question on whether the EU's digital strategy will be effective entails the more radical problem of whether the top-down rules of such strategy have been properly designed to address the speed of technological innovation and the futureproofing of the law. Technology can make legal regulation obsolete in a few years. The EU e-money Directive 46 from 2000 is a good example of how the regulatory claims of the law may fail vis-à-vis digital innovation. Soon after the implementation of the Directive, which aimed at expanding traditional forms of centralization to online interaction, new forms of payment, such as PayPal, made the legal regulation obsolete: the EU legislators in Brussels had to amend themselves with a new Directive, n. 110 from 2009.

Scholars have extensively debated the ways in which lawmakers can aim to prevent risks of obsolescence and inefficacy (Koops et al., 2006; Reed, 2012; Pagallo, 2017). This is the prerequisite of any Brussels effect. For example, lawmakers can provide instructions for legal compliance, as occurs with Art. 7 of the DMA on "compliance with obligations for gatekeepers." In other regulations, such as the GDPR, the futureproofing of the law has recommended a coregulatory model of

legal governance pursuant to the accountability principle of Art. 5. Since the law should not be often revised to keep the pace of technological innovation, nor hinder such innovation with its own provisions, Art. 5 of the GDPR establishes the principles that have to be followed by data controllers and the outcomes that should be abided by them. At the same time, Art. 5 of the GDPR leaves up to data controllers how they should attain such ends through forms of self-regulation, e.g., via their "organizational measures" (Art. 5(1)(f)). Art. 7 of the DMA seems to follow suit: "The gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety."

Such techniques of legal regulation are related to another key factor for the success of the EU's digital strategy that current debates on digital sovereigns, digital constitutionalism, or the Brussels effect tend to overlook. The more focus is on powers of alleged digital sovereigns, new digital rights, or new extraterritorial impacts of EU regulation, the less scholars pay attention to risks of legal fragmentation. To be sure, this risk is not new, although it could be exacerbated by the speed of technological innovation and the set of acts, policies, and proposals of EU law summed up with Table 1 above. Risks of fragmentation have been denounced since the inception of the GDPR (Mayer-Schönberger & Padova, 2016). By devolving powers back to MS in some crucial fields of today's data-driven societies, such risks have materialized in medical research (Aurucci, 2019), open science (Paseri et al., 2021), big data processing (Pagallo, 2018), and more. Although the GDPR has aimed to address these risks using coordination mechanisms and rules on procedural regularity, as in Articles 60, 61, 75(4), and 97(2)(b), the revision of such norms is in the current agenda of the EU institutions. Moreover, further norms on coordination have been adopted in the set of new acts for the governance and regulation of a data-driven society at the EU level.

These rules on procedural regularity and the use of coordination mechanisms, that is, what scholars dub as the 'secondary rules' of the law, play a critical role to determine whether the hard tools of the law will be effective. This is the part of the EU's digital strategy that regards the functioning and organization of the legal system with its norms of change, adjudication, and competence, often overlooked by current debates on the digital strategy of the EU institutions. What is at stake with the EU's digital strategy does not only concern power and control over data and information, rights of individuals, or extraterritorial effects of legislation, but also coordination and cooperation, as much as convergence on regulatory options among multiple jurisdictions. After the top-down rules of EU law under scrutiny in this section, what are the "secondary rules" at work with the digital strategy of the EU institutions?

3 Coordination, Cooperation, and Convergence

The analysis has dwelt so far on the rules of hard law, namely, the top-down commands and instructions of legislators, as regard either the current fight for control over data and information among multiple regulatory systems (digital sovereignty),

or new rights and duties for the protection of individuals (digital constitutionalism), or how these normative acts may unilaterally impact the rest of the world, e.g., market and jurisdictions (Brussels effect). The aim of this section is to complement these analyses with the other side of the coin on the politics of data in EU law. Rather than top-down provisions of hard law, the focus is on the role that mechanisms of coordination, models of cooperation, and convergence of regulatory approaches play in this context.

3.1 Mechanisms of Coordination

The role of coordination mechanisms can hardly be overestimated in most kinds of legal governance. As regard the top-down commands of legislators and their enforcement, such coordination mechanisms set up the ways in which public agencies, authorities, and institutions interact on the basis of the rules on competence, adjudication, and harmonization of the hard rules of the law. The aim is to strengthen the functioning of the system, while preventing risks of fragmentation, through the secondary rules-based mechanisms of coordination. Efforts at coordination play a critical role in most proposals of data governance and technological regulation in EU law. Such efforts may regard the harmonization of manifold pieces of legislation. In the AIA, for example, the new provisions on high-risk systems shall be harmonized with Regulation (EU) 2017/745 and Regulation (EU) 2017/746 on medical devices (Art. 47(6)); with Directive 2013/36/EU on the use of AI systems by credit institutions (Art. 9(9)) or with the new obligations and liability regime of the DMA (see above Sect. 2). Following the recommendation of scholars (Floridi et al., 2018; Pagallo et al., 2019a), the AIA also sets up a new European AI Board (Art. 56 ff.), to "coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation."

The functioning of coordination mechanisms does not only concern, however, public agencies and authorities, or international cooperation. Rather, coordination may regard the interaction between the public sphere and private actors. Scholars have stressed the strategic role of collaborations and alliances in critical fields of today's data-driven societies, such as the cloud and semiconductors, e.g., the Chips Act proposed in February 2022. In these fields, "collaboration in partnerships and alliances is the name of the game" (Timmers, 2022). Such forms of collaboration, partnerships, and alliances hinge on the coordination mechanisms set up by lawmakers through the secondary rules of the system. Going back to the EU Chips Act, the industrial-technological collaboration plan of the act includes a Joint Undertaking, as much as a regulatory toolbox to tackle supply-shortage risks of semiconductors that should be implemented through the coordination mechanisms set up with Art. 1(1)(c), Art. 14(4), and Art. 23(4), in accordance with the objectives of the Act (i.e., 1.4.2.3, at 63).

Section 2 already mentioned some of the new regulatory approaches endorsed by the EU lawmakers to tackle the challenges of technology through the accountability principle of the GDPR. This approach to legal governance can be traced back to

the Audiovisual Media Services Directive (AVMSD) and its Recital 44, according to which (Directive 2010/13/EU), co-regulation provides in its minimal form "a legal link between self-regulation and the national legislator… In co-regulation, the regulatory role is shared between stakeholders and the government or the national regulatory authorities or bodies." Further examples of co-regulation in EU law and its politics of data include the 2017 policy on better and smart regulation, and some technical developments of the EU Better Regulation scheme for interoperability (TOGAF, 2017), that fit like hand into glove with work of standardisation agencies. They include NIST-800–53 from 2013 and NIST-800-63C from 2016, together with ISO/IEC 27,002 and 27,001 on security and privacy controls for Federal Information Systems and Organizations. Along the same lines, this co-regulatory approach is consistent with some governance models in the business field, such as the COBIT2019 framework launched by ISACA and the Enterprise Architecture model, which aims to align management information systems with business interests (Pagallo et al., 2019b).

All these coregulatory options that work between the top-down commands of lawmakers and bottom-up activities of stakeholders depend on the functioning of coordination mechanisms and meta-rules of 'procedural regularity' (Pagallo, 2017). The secondary rules of the law cover all possible "legal links" and levels of engagement with private actors and stakeholders: from simple information to consultation, involvement, collaboration, down to delegation of legal powers through forms of experimentalist governance (Saber & Zeitlin, 2008), or derogation and open access (Du & Heldeweg, 2019). These legal experimentations include the creation of legally deregulated zones for the empirical testing and development of AI and emerging technologies. The Japanese government has created a number of such special zones, or *Tokku*, since the early 2000s (Pagallo, 2017). The European Commission has followed suit with Art. 53 of the AIA on regulatory sandboxes "in support of innovation" (Title V of the Act). The aim of such different levels of engagement is not only to strengthen the functioning of the system, by providing flexibility through mechanisms of coordination. The engagement of private actors and stakeholders in the decision-making process often represents the only way in which the law can tackle the normative challenges of digital technologies. Such challenges include the intent of several EU initiatives, plans, and policies on data governance, open science, green deal, or circular economy, to fully attain benefits and opportunities brought forth by digital technologies (Pagallo & Durante, 2022). Rather than misuses or overuses of data, of AI systems, or of other emerging technologies, the threat is posed by their possible underuse and corresponding opportunity costs. Since this is another crucial aspect of today's politics of data that most discussions on digital sovereignty, digital constitutionalism, or the Brussels effect tend to overlook, the next step of the analysis has to do with the role that cooperation plays in this context. What is the state-of-the-art in EU law?

3.2 Methods of Cooperation

There is a full array of initiatives and policies of EU law that aim to strengthen the re-use, sharing, and pooling of data essential to the flourishing of today's data-driven societies. They include the DGA, the EU DS, and the ODF. Such initiatives

and policies hinge on methods of cooperation, since the aim is to tackle the wrong reasons why useful technologies are exploited far below their full potential, or are not used at all due to public distrust, greed of both public and private data keepers, bureaucracy, lack of infrastructures, and more (Pagallo & Durante, 2022). In EU law, these initiatives or policies are either "horizontal" or "vertical." As regards the "horizontal approach," consider the aim of the DGA to "increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data sharing," in accordance with two models of cooperation. They are at work with the notification regime for data sharing providers set up in Chapter III of the proposed regulation, and the registration mechanism for "data altruism (data voluntarily made available by individuals or companies for the common good)," set up in Chapter IV of the DGA. As regards the "vertical approach," the European Commission's effort to enable the digital transformation of healthcare in the digital single market, i.e., the DHC, clarifies how this approach works in a specific legal sector. In July 2020, the Commission relaunched the e-health stakeholder group initiative, related to "all umbrella organisations/associations with a European outreach, representing the following sectors/groups: the health tech industry, patients, healthcare professionals and the research community" (EC, 2020). The intent is to "support the Commission in the development of actions for the digital transformation of health and care in the EU," providing advice and expertise, in particular, to enable the digital transformation of healthcare in a data-driven society. The EHDS only covers a part, although important, of such challenge as regard the design and functioning of e-health record systems through a mandatory self-certification scheme for such EHR systems.

The initiatives, policies, and normative acts that hinge on cooperation do not mean that all problems are solved: current societies, also but not only in the EU, often do not use AI and other emerging technologies that could be fruitfully employed to reduce polluting emissions, to strengthen the circular economy**,** to build more gender inclusive communities, or to improve the quality of life through personalized medicine and healthcare (Pagallo, 2022). The underuse of digital technologies entails that which economists dub as opportunity costs (Palmer & Raftery, 1999), namely, how much it costs not to use something or someone for professional reluctancy, bureaucracy, business greediness, or people's credulity in the era of no-vax conspiracies. In 2019, the European Parliament denounced the risk of AI underuse as a major threat: "missed opportunities for the EU could mean poor implementation of major programmes, such as the EU Green Deal, losing competitive advantage towards other parts of the world, economic stagnation and poorer possibilities for people" (EP, 2019). A similar risk has been stressed by such international organizations, as the (G20, 2019), the (OECD, 2019), or the (WHO, 2020). The problem is not whether but how much the underuse of AI and of other data-driven technologies costs our societies, and how the law should address the phenomenon.

In 2022, the Commission and the Parliament have vividly debated the impact assessment of the costs related to the implementation of the AIA. Similar debates and assessments have occurred with the GDPR as well. It is thus remarkable that neither lawmakers and institutions nor scholars and legal experts have fully addressed the "threat of AI underuse." The reason for this silence on the

opportunity costs of AI and how to legally tackle the phenomenon may depend either on the novelty of the challenge due to the breath-taking pace of technological innovation, or due to the fact that the focus has simply been on more popular topics, i.e., misuses or overuses of technology, rather than an 'invisible' underuse. There is little academic attention to why most efforts of legislators and public agencies, according to their own opinion (EP, 2019), have fallen short in fighting the underuse of AI. Although, over the past years, scholars have discussed new models of legal governance for the regulation of both bad and good uses of data-driven technologies, it remains unclear how to improve current policies and acts of lawmakers as regard the wrong reasons why today's societies underuse fruitful digital applications. New ways of legal cooperation have been adopted by the EU institutions with the DHC, the DGA, and some variants of the coregulatory model of EU law for green strategies and the circular economy. This approach seems reasonable because the legal fight against technological underuse and its opportunity costs cannot be enforced in a top-down way, i.e., by command, act, or decree. Since the drivers of technological underuse include "public and business' mistrust in AI, poor infrastructure, lack of initiative, low investments, or, since AI's machine learning is dependent on data, from fragmented digital markets" (EP, 2019), the focus should be on the procedural norms of coordination and cooperation set up in EU law, e.g., Chapter IV of the DGA. Scholars should examine how much these norms are effective, eventually suggesting how such acts of EU law can be ameliorated.

Such assessment, however, recommends complementing previous remarks on the enforcement, design, and extra-territorial effects of EU law with subtler forms of evaluation for the status of adherence to the regulatory provisions of the system. The examples of the GDPR, of the DGA, or of policies against the underuse of AI in the health sector show a more complex issue than the traditional stance, according to which either the legal agent is compliant, or not. Rather than 0 s and 1 s, focus should be on more nuanced assessments that distinguish between ideal, sub-ideal, and non-compliant statuses of legal agents (Lu et al., 2008) or between "good," "ok," or "bad" compliance (Morrison et al., 2009) down to more fine-grained views that distinguish between average compliance, reasonably high compliance, very high compliance, and full compliance (Hashmi et al., 2018). The binary alternative of compliance or non-compliance does not provide any useful information for the assessment and improvement of such institutional initiatives, as legal experimentation by open access *à la* DGA (Chapter III), by derogation *à la* AIA (Art. 53), by coregulation *à la* GDPR (Art. 5), etc. The "popularity" of the registration mechanisms for data altruism of the DGA, or the "efficacy" of current policies against the underuse of AI through methods of cooperation, should be finetuned between 0 and 1 to determine how much these norms have been effective in tackling the opportunity costs of technology. I esteem the opportunity costs for the underuse of AI systems in the public health sector in Italy from 1 up to 2% of its gross domestic product, including the "shadow prices" of the economy (Pagallo, 2022). Whether this part of the EU's digital strategy will succeed appears as crucial as current debates on the binding rules of EU law discussed in the previous section of this paper.

3.3 Unexpected Convergences

How EU law and other jurisdictions interact has been examined so far through the lens of discussions on digital sovereignty (e.g., control over data in a data-driven society), digital constitutionalism (e.g., new rights against transnational corporations), and the Brussels effect, namely, the extra-territorial impact of EU law. Such stances shall be now complemented with a fruitful exercise in comparative law. Transplants and receptions are the bread and butter of experts in the field (Graziadei, 2006; Watson, 1993). Interestingly, such dynamics of transplants, receptions, or rejections can occur unexpectedly. Two cases are particularly instructive in this context. They regard current trends of legal convergence in health law, data protection, and consumer law that complement current discussions on the enforcement, design and extra-territorial effects of EU law.

The first case refers to the activities of the European Commission in the e-health sector vis-à-vis the risk of AI underuse. Other jurisdictions have adopted a similar approach. In Singapore, the Medical Devices Branch of the Health Sciences Authority (HSA) has developed methods of coordination and cooperation with most relevant stakeholders to ensure the rapid implementation of new AI systems for medicine and health, from research labs to hospitals wards (Blasiak et al., 2020). In Australia, the "Stakeholder Engagement Framework" of the Department of Health has fleshed out five principles of engagement that should address cases of technological underuse: from simple information to consultation, involvement, collaboration, and finally, delegation of legal powers to stakeholders (AG, 2017). In the US, the regulation of software as a medical device ('SaMD') illustrates how soft law and mechanisms of cooperation complement the provisions of hard law, through the powers of the Federal Drug Administration, or "FDA," to examine applications, develop policies, publish guidance, or ask for feedback (Pagallo, 2022). This convergence of regulatory approaches is unsurprising: the more technology grows complex, the less top-down and bottom-up solutions look fruitful, so that the attention has increasingly been turned into the coregulatory options that lie in between. Several legal systems and their public agencies have converged, often independently one from the other, in adopting methods of coordination and models of cooperation, because this appears the only way to address some normative challenges of technological innovation, such as the underuse of AI in the health sector.

The second case brings us back to the GDPR and Italy, land of legal transplants, and rejection crises. Three attempts of the Italian lawmakers provide the necessary framework for the analysis of current trends in data regulation. First, on 22 September 1988, Italy adopted a new code of criminal procedure, aiming to substitute the previous inquisitorial system with an adversarial system, typical of the common law tradition. Then, it was the turn of data protection. The 1995 EU Directive n. 46 was implemented with the Italian Act n. 675 from 1996. Finally, in January 2010, after 6 years of parliamentary work and discussions, a further transplant occurred with such a powerful US legal tool, as the class actions, implanted into the Italian Consumer Code with Art. 140 *bis*. Whereas it may be too early to determine whether or not the rules on the new Italian class actions shall be deemed as a success story of

legal reception, the two previous transplants can be grasped as the opposite sides of a spectrum. At one end, there is the failure, or rejection crisis, of the adversarial system: several new provisions on the role of the parties, their powers, the notion of procedural truth, etc., contrasted with some principles of the Italian constitution and the Constitutional Court in Rome had to declare invalid the core of the reform. At the other end of the spectrum, I may dare to say that the adoption of the EU data protection rules in Italy has been a success. After all, the word privacy, which is often used as a synonym of data protection in Italy, turned out to be a new Italian word since the mid 1990s (although pronounced in the American, rather than British way).

Still, even the GDPR has its problems. Some of them, e.g., the fragmentation of the system, have been mentioned above in Sects. 2 and 3.2. In the US law, scholars discuss whether their national and federal law could learn something from the EU's shortcomings and overtake its data policies (Hartzog & Richards, 2020). Others stress persisting differences due to an American-style transparency law tradition, which includes the California Consumer Privacy Act (CCPA), from 2020 (Kaminski, 2020). Such crucial differences should not overlook, however, some issues that EU and US law have in common, namely, how to safeguard the collective, rather individual level of protection that the law should guarantee vis-à-vis the challenges of (big) data-driven technologies. Computational models of data mining and profiling techniques assemble individuals in connection with certain educational, occupational or professional capabilities, or social practices (e.g., a religion), and social characteristics (e.g., an ethnicity). The aim is to predict people's behaviour, and include or exclude individuals from a particular service, product, or credit. As a result, individuals are targeted as members of a group, although they can ignore even being a part of such group. By regarding types, rather than tokens — and hence groups, or aggregates, rather than individuals – big data techniques are thus affecting the traditional viewpoint of EU law, according to which the challenges of data-driven technologies mostly revolve around the protection of individuals (and not group rights).

Scholars have time and again insisted on this drawback of EU law (Taylor et al., 2017), which the EU institutions find hard to address. It is noteworthy that some MS of the Union have reacted to the shortcomings of EU law, through the rulings of their Courts. Going back to the Italian legal transplants, some loopholes of the GDPR, e.g., the collective dimension of protection for data privacy pursuant to the limited associative rights of Art. 80, have been filled with the class actions of the Consumer Code. With the words of the Administrative Tribunal in Rome, from January 2020, this approach offers a powerful "view of the potential inherent in the exploitation of personal data, which can also constitute an 'asset' available in a negotiating sense, susceptible of economic exploitation… In addition to the protection of personal data as an expression of a right of the individual's personality, as such subject to specific and non-waivable forms of protection, such as the right to withdraw consent, access, rectification, oblivion, there is also a different field of protection of the data itself, intended as a possible object of a sale, put in place both between market operators

and between them and the interested parties."[1] Some months later, in March 2021, the Council of State, that is, the highest administrative Court in Italy, confirmed this part of the ruling.[2]

Against this backdrop, we can appreciate how an American legal tool (i.e., class actions) has been transplanted into a national legal system (i.e., the Italian consumer code), in order to complement the provisions of a quasi-federal legislation, such as the GDPR of EU law. The gist of this "imitation game" in comparative law is that "Brussels effects" may work both ways: no incompatibility exists between consumer law and data protection, since they should be grasped as complementary. Depending on the circumstances of the case, individuals and associations may lodge complaints either before their data protection and privacy authorities, or before their national competition and market authorities, or both. There is no such alternative between US law ("we have our data") and EU law ("we are our data"). Rather, groups and individuals can protect their data for personal and economic reasons, as much as occurs in US law, through the powerful tool of class actions, e.g., Art. 140 *bis* of the Italian Consumer Code, or through the weak associative mechanisms of Art. 80 of the GDPR. This conclusion fits hand into glove with the ruling of the European Court of Justice's Third Chamber on 28 April 2022.[3]

4 A Twin Challenge

In the Explanatory Memorandum of the AIA, the European Commission presented the green and digital transformations of our society as a "twin challenge." The metaphor can fruitfully be transplanted in this context to grasp the challenges of the EU digital strategy as well. Such challenges regard, on the one hand, the hard tools of the law and top-down provisions of lawmakers against misuses and overuses of technology, on the other hand, forms of coordination and cooperation against underuses of technology and their opportunity costs.

The twin challenge of the EU institutions has been illustrated with multiple stances, or levels of abstraction, through which scholars aim to describe, examine, and argue about the politics of data in EU law. Section 2 dwelt on three of these levels of abstraction: the stances of digital sovereignty, digital constitutionalism, and the Brussels effect. The aim was to stress both the merits and limits of these points of view. They shed light on crucial issues for the politics of data in EU law that revolve around the

[1] TAR Lazio, first section, 10 January 2020, n. 15,275/2018, no. 6 of the ruling.

[2] Consiglio di Stato (sixth Section), ruling no. 02631/2021 (REG.PROV.CO), from 31st March 2021.

[3] See the EU Court of Justice (third camber), Case C-319/20, according to which "a consumer protection association" is "able to bring legal proceedings, in the absence of a mandate… and independently of the infringement of the specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions." The case refers once again to Facebook, now Meta Platforms (Ireland), against the German Federal Union of Consumer Organisations and Associations. This has been my viewpoint over the past years: see (Pagallo, 2020).

Table 2 Data politics in EU law (one side of the coin)

Level of abstraction	What is at stake	What is missing
Digital sovereignty	Power over data in data-driven societies	Subsidiarity at work: balance of power between EU and MS
Digital constitutionalism	New rights	Habeas data
The Brussels effect	Extra-territorial impact of law	Engagement

Table 3 Data politics in EU law (walking through the other side)

Level of abstraction	What is at stake	Open issues
Mechanisms of coordination	Harmonization or fragmentation	GDPR, AIA, DAct, etc
Models of cooperation	The underuse of data-driven technologies	DHC, GDA, ODF, etc
Spontaneous convergences	Filling legal gaps	Group rights, rejection crises

top-down rules of hard law, and still, these perspectives seem to presuppose that some problems are solved, when they are not. Table 2 illustrates the results of Sect. 2:

Section 3 complemented the analysis on the politics of data in EU law with three further levels of abstraction. The aim was to address matters of power, rights and duties, and legal effects among jurisdictions with three further stances on legal coordination, cooperation, and convergence among legal systems. The overall aim was to cast light on that which is often overlooked, but still plays a key role in today's data politics. Table 3 illustrates the results of Sect. 3:

Against the features of Tables 2 and 3, I am ready to concede that further variables of the legal analysis would merit a space of their own. For example, as regard the hard tools of EU law under scrutiny in Sect. 2, the paper did not scrutinize fields that are critical for the assessment of current data policies in Europe, e.g., cybersecurity and AI systems for immigration policies. Likewise, as concerns the coordination mechanisms and models of cooperation illustrated in Sect. 3, the paper did not examine the role of further legal means of governance and regulation, such as the soft law of public agencies that often play a decisive role in the politics of data: the opinions and recommendations of the EDPB in data protection law, EASA in civil aviation law, EMA in health law, etc. However, such legal cases and sources of regulation either fall under the dichotomies of this paper, e.g., hard law and soft law, or they add no indispensable information to address the final issue of this paper. By going back to the question of its title, 'will EU law succeed'?

5 Conclusions

The great economist Kenneth Galbraith used to say that the only function that "predictions" have is to make astrology respectable. The question on whether EU law may succeed in governing societies that depend on data and information as

their vital resource should not entail prophetic powers. It is still unclear, however, how the final version of several proposals of the Commission will look like after the institutional round of amendments and discussions at the European Parliament and the Council. Whether such acts and proposals of EU law will be successfully enforced in the internal digital market, or adopted, or imposed in other jurisdictions, thus remain open problems.

Yet, drawing on the differentiations of legal theory and work on governance of technological regulation, the analysis has shown that such a question — whether EU law will attain its own aims (and those of its advocates) — entails two different kinds of issues. The metaphor on the "twin challenge" of the EU digital strategy is instructive since it reminds us of this crucial differentiation. Although the normative challenges of data and data-driven societies, such as the misuse, overuse, and underuse of technology, are closely related to each other like two offspring born at one birth, the metaphor also suggests that twins have problems of their own. The analysis has provided guidance for fleshing out such differences. The question on whether EU law will be effective and successful either regards the issues of Table 2, or conversely, of Table 3 of this paper. There is no further alternative. In the case of Table 2, the focus was on the EU hard laws and its provisions on the governance and regulation of data-driven societies with the corresponding matters of power and enforcement, rights, and legal effects. This is the bread and butter of current debates on digital sovereignty, digital constitutionalism, and the Brussels effect. Vice versa, in Table 3, the focus was on that which is often overlooked by such debates, namely, the coregulatory and cooperative initiatives and policies of EU law that shall exploit all benefits of technology. The paper illustrated why the risk of technological underuse for environmental protection, medical care, circular economy, open science, gender-inclusiveness, etc., is as much as threatening as the risk of technological overuse or misuse. Furthermore, the attention was drawn to subtler forms of evaluation for the status of adherence to the regulatory provisions of the system that should complement the traditional stance, according to which either legal agents are compliant, or not. As stressed above in Sect. 3.2, the assessment and improvement of such institutional initiatives, as legal experimentation by open access *à la* DGA, derogation *à la* AIA, or coregulation *à la* GDPR, should determine the "popularity" of the registration mechanisms for data altruism of the DGA, the "efficacy" of current policies against the underuse of AI through methods of cooperation, etc. Therefore, where and how should EU law ever succeed?

By considering critical differences on misuses, overuses, and underuses of technology, the panoply of acts, proposals, and initiatives of the EU institutions recommends preventing generalizations; however, the threat of technological underuse seems more challenging than the success of current EU policies against misuses and overuses of technology. The conjecture rests on the old Aristotelian meaning of politics and the corresponding aim of the law to strike a balance among the multiple regulatory systems in competition out there: Sects. 3.2 and 3.3 above stressed a relative lack of experience that EU law has with models of cooperation. This lack of experience goes hand-in-hand with the difficulty of addressing causes of underuse that depend either on the invisibility or on the novelty of the phenomenon. Consider

the new role of public agencies and authorities that should work together with all relevant stakeholders to find solutions for the open problems of the field. The goal often requires a change of mentality that can be as difficult to achieve as regulating the challenges of technology.

Underusing digital technologies may cost even more than employing them too much, or for bad purposes. In addition to the hard tools of EU law against misuses and overuses of digital technologies, scholars should thus be attentive to this ongoing threat of technological underuse, and how to overcome it. The paper has illustrated efforts of EU law on this side of data politics, providing a list of normative acts and proposals that shall be under constant scrutiny. It would be a terrible mistake to underestimate the opportunity costs of technology.

Author Contribution Not applicable.

Funding Open access funding provided by Università degli Studi di Torino within the CRUI-CARE Agreement.

Data Availability Not applicable.

Materials and/or Code Availability Not applicable.

Declarations

Ethics Approval Not applicable.

Consent of Publication Not applicable.

Competing Interests Not applicable.

References

Aristotle. (2000). *The Nicomachean Ethics*, trans. and ed. by R. Crisp, Cambridge University Press.

Arner, D. W., Castellano, G., Selga, E. (2022). The transnational data governance problem, *Berkeley Technology Law Journal*, University of Hong Kong Faculty of Law Research Paper No. 2021/039. https://doi.org/10.2139/ssrn.3912487.

Aurucci, P. (2019). Legal issues in regulating observational studies: The impact of the GDPR on Italian biomedical research. *European Data Protection Law Review, 5*(2), 197–208.

Australian Government's Health Department (AG). (2017). *Stakeholder engagement framework* (last updated November 2018), Retrieved from: Apr 2022 https://www.health.gov.au/resources/publications/stakeholder-engagement-framework.

Blasiak, A., Khong, J., Kee, T. h. (2020). CURATE.AI: Optimizing personalized medicine with artificial intelligence, *SLAS Technology*, 25(2): 95–105.
Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review, 107*(1), 1–68.
Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society, 21*(10), 2305–2322.
De Gregorio, G. (2020). The rise of digital constitutionalism in the European Union, *International Journal of Constitutional Law*, 41–70.
Du, H., & Heldeweg, M. A. (2019). An experimental approach to regulating non-military unmanned aircraft systems. *International Review of Law, Computers & Technology, 33*(3), 285–308.
European Parliament (EP). (2019). *Artificial intelligence: Threats and opportunities*, press release, https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities (updated March 29, 2021; last accessed March 24, 2022).
European Commission (EC). (2020). The eHealth Stakeholder Group is relaunched, 13 July 2020, available at https://digital-strategy.ec.europa.eu/en/library/ehealth-stakeholder-group-relaunched (last accessed September 20, 2022).
Floridi, L. (2014). *The Fourth Revolution*. Oxford University Press.
Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, V., & Vayena, E. (2018). AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*(4), 689–707.
G20. (2019). *The G20 Tokyo AI Principles*, https://www.g20-insights.org/related_literature/g20-japan-ai-principles/.
Graziadei, M. (2006). Comparative law as the study of transplants and receptions, 442–461. In M. Reimann, R. Zimmermann (eds.), *The Oxford Handbook of Comparative Law*, 2nd ed., Oxford.
Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *Boston College Law Review, 61*(5), 1689–1761.
Hashmi, M., Casanovas, P., & de Koker, L. (2018). Legal compliance through design: Preliminary results of a literature survey. *TERECOM2018@ JURIX, Technologies for Regulatory Compliance*. http://ceur-ws.org/Vol-2309/06.pdf.
Kaminski, M. (2020). Law and technology: A recent renaissance in privacy law. *Communications of the ACM, 63*(9), 24–27.
Koops, B.-J., et al. (2006). Should ICT regulation be technology-neutral? In B. J. Koops (Ed.), *Starting points for ICT regulation: Deconstructing prevalent policy one-liners* (pp. 77–108). TMC Asser.
Lu, R., Sadiq, S., & Governatori, G. (2008). Measurement of compliance distance in business processes. *Information Systems Management, 25*(4), 344–355.
Madiega, T. (2020). *Digital sovereignty for Europe*, EPRS: European parliamentary research service. Retrieved from https://policycommons.net/artifacts/1336893/digital-sovereignty-for-europe/1944437/ on 04 Sep 2022. CID: 20.500.12592/5n1gmm.
Mayer-Schönberger, V., & Padova, E. Y. (2016). Regime change? *Enabling Big Data through Europe's New Data Protection Regulation, Columbia Science and Technology Law Review, 17*, 315–335.
Mitsilegas, V. (2022). *EU criminal law* (2nd ed.). Hart.
Morrison, E., Ghose, G., Aditya, K., & Koliadis, G. (2019). Dealing with imprecise compliance requirements, *Proceedings of the 2nd International Workshop on Dynamic and Declarative Business Processes (DDBP 2009)*, IEEE Computer Society Press.
OECD. (2019). *AI Principles*, https://oecd.ai/en/ai-principles.
Palmer, S., & Raftery, J. (1999). Opportunity cost. *BMJ, 318*(7197), 1551–1552.
Pagallo, U. (2013). Online security and the protection of civil rights: A legal overview. *Philosophy and Technology, 26*, 381–395.
Pagallo, U. (2015). Good onlife governance: On law, spontaneous orders, and design. In L. Floridi (Ed.), *The Onlife Manifesto* (pp. 161–177). Springer.
Pagallo, U. (2017). The legal challenges of big data: Putting secondary rules first in the field of EU data protection. *European Data Protection Law Review, 3*(1), 34–46.
Pagallo, U. (2018). Algo-rhythms and the beat of the legal drum. *Philosophy & Technology, 31*(4), 507–524.
Pagallo, U. (2020). The collective dimensions of privacy in the information era: A comparative law approach, *Annuario di diritto comparato e studi legislativi*, SKU: 9920179006.

Pagallo, U. (2022). *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Mimesis, Milano.

Pagallo, U., & Quattrocolo, S. (2018). The impact of AI on criminal law, and its twofold procedures, in W. Barfield and U. Pagallo (eds.), *The research handbook of the law of artificial intelligence*, Elgar Cheltenham, UK e Northampton, MA., USA.

Pagallo, U., Aurucci, P., Casanovas, P., Chatila, R., Chazerand, P., Dignum, V., Luetge, Ch., Madelin, R., Schafer, B., & Valcke, P. (2019a). *AI4people – On good AI governance: 14 priority actions, a SMART model of governance, and a regulatory toolbox*, presented at the European Parliament, Brussels, on November 6th, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486508 (accessed on April 3, 2022).

Pagallo, U., Casanovas, P., & Madelin, R. (2019b). The middle-out approach: Assessing models of legal governance in data protection, Artificial Intelligence, and the Web of Data. *Theory Pract. Legis., 7*, 1–25.

Pagallo, U., & Durante, M. (2022). The good, the bad, and the invisible with its opportunity costs, *J,* 5(1): 139–149.

Paseri, L., Varrette, S., & Bouvry, P. (2021). *Protection of personal data in high performance computing platform for scientific research purposes, Annual Privacy Forum, 123–142*. Springer.

Reed, C. h. (2012). *Making Laws for Cyberspace*. Oxford University Press.

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*.

Saber, C. F., & Zeitlin, J. (2008). Learning from difference: The new architecture of experimentalist governance in the EU. *European Law Journal, 14*(3), 271–327.

Sajó, A., & Uitz, R. (2017). *The constitution of freedom: An introduction to legal constitutionalism*. Oxford University Press.

Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). *Group privacy: New challenges of data Technologies*. Springer.

Timmers, P. (2022). *Strategic autonomy tech alliances*, FEPS, April.

TOGAF. (2017). An introduction to the European Interoperability Reference Architecture (EIRAC) v2.1.0, 2017. Available at https://joinup.ec.europa.eu/sites/default/files/distribution/access_url/2018-02/b1859b84–3e86–4e00-a5c4-d87913cdcc6f/EIRA_v2_1_0_Overview.pdf.

Waldron, J. (2012). Constitutionalism: A skeptical view (May 1, 2012). *NYU School of Law, Public Law Research Paper No. 10–87*, Available at SSRN: https://ssrn.com/abstract=1722771.

Watson, A. (1993). *Legal transplants: An approach to comparative law* (2nd ed.). University of Georgia.

WHO. (2020). World Health Organization's *AI for Good*, https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/who/.