1

Data at the Boundaries of (European) Law: A First Cut

Mariavittoria Catanzariti and Deirdre Curtin

1. Introduction

In Europe, data-driven governance, both public and private, has taken root in myriad ways. Legislative responses echo and follow practice by both public and private actors, and grapple with the complex ways they intermingle both at the national level as well as that of the supranational European Union (EU) level. The EU has been itself 'mimetic' in certain legislative trajectories it has followed in the past decade and more.[1] In certain fields its stance is optimistic as to the role that data gathering, retention, and access can and should play in European governance. Banks play a role in combatting terrorist financing, airline carriers assist in tracking free movement, internet intermediaries in supporting law enforcement, and private companies receive support when combatting fraud. The extent to which Europe's governance has become data-driven is striking. The EU itself sees some of its data regulatory measures as truly world leading.[2] The most obvious example of this is in the field of data protection (GDPR) but more recent legislative initiatives place far reaching public obligations on private actors, for example, in the security field (TERREG), and also notably in the EU's draft regulation for artificial intelligence (the AI Act) as well as the Digital Services Act.[3] In these examples, a certain optimism is detected in the

[1] De Hert, Chapter 4, this volume.

[2] Kuner, 'The Internet and the Global Reach of EU Law', in M. Cremona and J. Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (2019); A. Bradford, *The Brussels Effect: How the European Union Rules the World* (2020) 131; Greenleaf, 'The "Brussels Effect" of the EU's "AI Act" on Data Privacy Outside Europe', 171 *Privacy Laws & Business International Report* (2021) 1, at 3–7; Svantesson, 'Article 3. Territorial scope', in C. Kuner, L. A. Bygrave and C. Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2019) 74.

[3] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', COM/2021/206 final; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC', COM/2020/825 final. On the role of private actors

Mariavittoria Catanzariti and Deirdre Curtin, *Data at the Boundaries of (European) Law: A First Cut* In: *Data at the Boundaries of European Law.* Edited by: Deirdre Curtin and Mariavittoria Catanzariti, Oxford University Press.
 DOI: 10.1093/oso/9780198874195.003.0001

underlying assumption that increased access to data will lead to better enforcement outcomes both at the European level and at the national level. It seems that data-driven Europe within and at the boundaries of European law has come squarely into its own.

The ambition (and practice) of the GDPR in particular is to be a regulatory model for the world.[4] While this effect should not be reduced to a unilateral exercise of EU power,[5] the fact remains that EU legislation in digital matters exerts direct and indirect influences on public and private actors around the world. Recent examples of this influence include the requirements that data controllers must observe when transferring data to non-EU jurisdictions not covered by an adequacy decision[6] and the frequent mention of the GDPR by legislators in various Latin American countries.[7] Institutional practice that has developed over many years in the field of EU external relations adopts individual country-specific adequacy rulings for third countries. This guarantees that third-country legislation/regulation is up to European standards and is required before data can be shared beyond the EU. This multiplication effect makes it very difficult for third countries to avoid negotiating arrangements that are basically EU law compliant. Ignoring or altering compliance brings with it the risk of the EU not agreeing to share data with them. This is at issue presently regarding the UK post Brexit, which announced its intention to move away from strict GDPR compliance (which it already adopted into its own legislation before its EU exit) for what it terms a more 'common-sense' approach. How this will fare in terms of the EU accepting its 'adequacy' will likely be a highly politicized and salient saga that could run over (many) years and will

in enforcing the AI Act, see Veale and Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act —Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach', 22 *Computer Law Review International* (2021) 97; Ebers, 'Standardizing AI—The Case of the European Commission's Proposal for an Artificial Intelligence Act', in L. A. Di Matteo, M. Cannarsa and C. Poncibò (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (2022). On the Digital Services Act as a mechanism for fostering the responsibility of private actors, see, e.g., Carvalho, Lima and Farinha, 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection', 3 *Revista de Direito e Tecnologia* (2021) 71.

[4] Data protection law has been proposed as a paradigmatic instance of the global impact of EU law: Bradford (n. 2). This impact of EU law beyond the physical borders of the Union has implications for the promotion of EU fundamental values and to the definition of its legislative boundaries: Kuner (n. 2).

[5] Schwartz, 'Global Data Privacy: The EU Way', 94 *New York University Law Review* (2020) 771.

[6] See further, European Data Protection Board, 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data' (2020).

[7] See for example, Bertoni, 'Convention 108 and the GDPR: Trends and Perspectives in Latin America', 40 *Computer Law & Security Review* (2021), 1.

have obvious implications also in the context of law enforcement and security data sharing as well as trade.[8]

Data sharing in the context of law enforcement and security by and to the EU is a subject about which considerably less has been written than on the GDPR (or only within highly specialized circles).[9] In substance it is a highly developed practice with its origins in soft law but more recently in some actual hard law. It is infused with optimism for the role of data and data interoperability in particular to thwart terrorism and assist in the arrest and prosecution of suspected criminals, not to speak of (illegal) immigrants. It is used both internally by the EU and its own institutions and agencies as well as by its Member States and externally with third countries under specific institutional arrangements (for example, by Europol with third countries).[10] Unlike the GDPR, it is a subject straddling the border of European law. Through specific regulations and international agreements (e.g. Terrorist Finance Tracking Programme (TFTP)) data sharing stands with one foot in European law, but with the other foot very much out in terms of how actual arrangements work in practice (non-regulatory interoperability—the so-called black box).

The debate on data within and beyond European law is also, given the nature of data, global, even if the solutions are often not global. Rather, they are national and increasingly supranational.[11] Part of what this book is about is

[8] Early signs of this politicization were seen when the European Parliament approved a resolution expressing a series of concerns about the then-forthcoming adequacy decision relating to the UK data protection regime: EP Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)). Since then, the British government has opened a public consultation on reforms to the UK data protection regime, with the stated goal of moving away from the general model of the GDPR: Department for Digital, Culture, Media & Sport, 'Data: A New Direction' (2021) Public Consultation.

[9] See for example, Galli, 'Interoperable Databases: New Cooperation Dynamics in the EU AFSJ?', 26 *European Public Law* (2020) 109; Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships', 8 *International Data Privacy Law* (2018) 52; Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU', 21 *Human Rights Law Review* (2021) 433; Dimitrova and Quintel, 'Technological Experimentation Without Adequate Safeguards? Interoperable EU Databases and Access to the Multiple Identity Detector by SIRENE Bureaux', in D. Hallinan, R. Leenes, and P. De Hert (eds), *Data Protection and Privacy: Data Protection and Artificial Intelligence* (2021) 217; V. Mitsegalis and N. Vavoula (eds), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives* (2021).

[10] F. Coman-Kund, *European Union Agencies as Global Actors. A Legal Study of the European Aviation Safety Agency, Frontex and Europol* (2018), at 231–249.

[11] See, for example, Council of Europe's modernized Convention 108 has been proposed as a compromise solution for a global data protection regime: Mantelero, 'The Future of Data Protection: Gold Standard vs. Global Standard', 40 *Computer Law & Security Review* (2021) 1. While there is a considerable overlap between the parties to Convention 108 and the members of the EU, the convention has nevertheless managed to extend its reach beyond the Union and beyond Europe itself: Makulilo, 'African Accession to Council of Europe Privacy Convention 108', 41 *Datenschutz und Datensicherheit* (DuD) (2017) 364. Nevertheless, Greenleaf, 'How Far Can Convention 108+ 'Globalise'? Prospects for Asian Accessions', 40 *Computer Law & Security Review* (2021) 1, argues that there is a considerable number of countries that would not be able to meet the accession standards for Convention 108.

indeed the specifically European take on how to regulate the use of data in binding legislation. This will be enforced through national and supranational executive power as well as in the courts and by supervisory authorities. This is not just GDPR-related. In fact, the GDPR is not at the centre of what we—the authors of this volume—analyse, as this has been done very extensively elsewhere. The core of what we wish to uncover does not merely relate to data protection and/or privacy but to underlying systemic practices and the implications for law as we understand it in a non-digital context.

Making wider European institutional and code practices visible in and around the EU, but not exclusively so, can contribute to a much wider debate on several salient issues of substance and structure. In our introductory chapter to this book, we wish to consider more broadly what it means to speak of data at the borders or boundaries of the law in general and in Europe. This constitutes a red thread that informs some of the specific choices made in individual chapters throughout the book that we return to in our last paragraph. We will first dissect the meaning of the words 'boundary', 'border', 'law', and 'data' before moving on to analyse the more general approach of the EU not only regarding specific (draft) regulations but also to the role of law more generally in the European integration process. We then finish with an evaluation of data-led law in the EU system and ask the following questions. What has data-led law meant for individuals in terms of their rights? What has it meant for institutions in terms of their accountabilities? What are the challenges facing the EU in this regard in the coming five or ten years? What are the more general global challenges in this regard?

2. Data from Boundaries to Borders

The idea of boundaries is inherent to legal rationality. The law in fact distinguishes an inside from an outside to define itself. It generally aims to shape a locked system in the sense that it limits itself with regard to other social systems and self-defines its scope and the remit of its relevance. Only the law says what the law is. The concept of boundary is thus quintessential to the concept of law. Boundaries of the law can be of various types and forms. The law not only asserts its authority with respect to what is non-law, but also within itself across

Consequently, it seems somewhat unlikely that Convention 108 will become a global standard in the near future.

different areas.[12] It constantly differentiates its functioning, rationales, and by-products in various modalities. Boundaries of the law lie in between the law and what the law excludes from itself or lie beyond its remit. Boundaries have a normative meaning, as they describe the way of being of the law in its positioning towards other relevant fields, such as politics, ethics, technology, and economy. They are not fixed and can change over time on different grounds as a measure of asserting authority or re-establishing order.[13] An obvious example is the legal concept of territory as the physical area where a specific legal order is established; another is the tension between deterritorialization and re-territorialization of legal spaces in times of crises, for example, the migration crisis or the securitization of Europe.[14] A logical starting point to define a boundary for the law is the use of language and the way definitions are built up. The law defines its own vocabulary. It is self-standing and autonomous. In terms of semantics, the fact that the law should be informed by the context that it aims to rule determines its own legal definition of the context as well as its own meaning or translation of reality into its own language.

This book mainly deals with a type of boundary that has profoundly shaped a new way of lawmaking: automation combined with personal data. In other words, this refers to the way algorithms make use of personal data to classify individuals, predict their behaviour, and make decisions about them.[15] It seeks to explore different layers of decision making using personal data—national, supranational, transnational—that are woven together with data-driven techniques and have differential impacts upon legal relationships and governance. In this data-driven field, the boundary of law and technologies is narrow and permeable, such that technology may replace the law. First, as one of our contributors, Hildebrandt (Chapter 2) has reminded us (in *Law for Computer Scientists and Other Folk*), legal design is not enough to ensure a legal disciplinary domain.[16]

The awareness that technological determinism may impair individual freedom of choice and information—e.g. the need to preserve human agency—makes urgent the integration of legal protection by design in human rights

[12] N. Luhmann, *The Differentiation of Society* (1982) 122.

[13] G. Popescu, *Bordering and Ordering the Twenty-first Century: Understanding Borders* (2011).

[14] See further: M. Fichera, *The Foundations of the EU as a Polity* (2018) at 132, 154; V. Squire, *Europe's Migration Crisis. Border Deaths and Human Dignity* (2020), at 15–42; J. Martín Ramírez, 'The Refugee Issue in the Frame of the European Security: A Realistic Approach', in J. Martín Ramírez and J. Biziewski (eds), *Security and Defense in Europe* (2020) 47.

[15] G. Sartor and F. Lagioia, *The Impact of the General Data Protection Regulation on Artificial Intelligence* (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (last visited 9 February 2022).

[16] M. Hildebrandt, *Law for Computer Scientists and Other Folk* (2020), at 267–270.

protection with research on and the architecture of data-driven systems.[17] Second, many areas where automation is applied and are currently not covered by the law in fact produce legal effects. Article 22(1) GDPR for example is explicit in its reach over decisions that produce 'legal effects concerning [the data subject] or similarly significantly affects him or her'.[18] As De Hert correctly points out in Chapter 4 this results in a lack of creativity: 'Is human intervention and the prohibition to use sensitive data all provided for by this provision that is needed to regulate profiling well?' It is then clear enough that data accuracy cannot be the exhaustive response to the lack of interpretability of an automated process, as explained by Hildebrandt: 'we should not buy into the narrative that proprietary software may be more opaque but will nevertheless be more accurate'.[19]

The transformation of human as well as of global relationships into data lies unquestionably at the crossroads of salient challenges for law and society.[20] Data may affect the legal dynamics in at least three ways: as the specific object of regulation; as a source of the law; and finally, as informing the functioning of legal patterns (not formally included in an actual law). These cases are examples of data-driven law but to varying degrees and in different ways. The first case specifically refers to regulatory models of data flows and data governance;[21] the second case relies on forms of personalized laws or tailored contracts targeting certain subjects;[22] and the third case is instead related to data-driven legal design combined with AI applications that are used in diverse areas of the law, such as predictive policing, insurance, and public administration.[23]

[17] See further on this distinction, ibid. 270–277 and 302–315.

[18] On the meaning of 'similarly significant' in the GDPR, see Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling', in C. Kuner, L. A. Bygrave, and C. Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 522.

[19] Hildebrandt, Chapter 2, this volume.

[20] S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power* (2019).

[21] The most relevant instruments for this volume's discussions are the GDPR (Regulation (EU) 2016/179, OJ 2016 L 119/1), the Law Enforcement Directive (LED: Directive (EU) 2016/680, OJ 2016 L 119/89), the Regulation on the free flow of non-personal data (Regulation (EU) 2018/1807, OJ 2018 L 303/59), the Open Data Directive (Directive (EU) 2019/1024, OJ 2019 L 172/56), and the Network and Information Security Directive (Directive (EU) 2016/1148, OJ 2016 L 194/1). To these we can add several ongoing legislative procedures: the Data Governance Act (Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance', COM/2020/767 final), recently adopted as Regulation (EU) 868/2022 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (hereinafter, Data Governance Act); the Digital Services Act (European Commission, COM/2020/825 final); and the AI Act (European Commission, COM/2021/206 final).

[22] Casey and Niblett, 'A Framework for the New Personalization of Law', 86 *University of Chicago Law Review* (2019) 333, at 335.

[23] K. Yeung and M. Lodge (eds), *Algorithmic Regulation* (2019).

The processing of huge amounts of data increasingly shapes the morphology of regulatory instruments. At the same time, algorithm-based regulation, and algorithmic personalization of legal rules (so-called granular norms) are instead one of the key portals through which data disruptively enters and modifies legal rationality. The collection of data inevitably acts as a new source for the law. What is at stake is not only the autonomy of the law in managing 'datafied' relationships and phenomena, but also the certainty of the law in its general applicability *erga omnes* and not only in relation to targeted/profiled subjects.

In terms of defining data in an operational fashion, a European perspective arguably adds value. The EU regulatory quest for a data strategy recently led to the very first definition of the term 'data' in a legal instrument. Both the Data Governance Act and the Data Act define data as 'any digital representation of acts, facts or information or any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording'.[24] The relevance of the digitalization itself represents the threshold of the law seeking to incorporate data into its domain. Data first of all sets the boundaries of the law, before a binary approach follows with data either personal or non-personal in nature. In recent years the regulatory tendency was indeed quite the opposite. Data protection reform, including the GDPR and its sister Law Enforcement Directive,[25] represent a truly monumental set of rules seeking to harmonize data privacy laws across Member States. Conversely, the Regulation on the free flow of non-personal data was merely a residual piece of legislation applicable only to data that is non-personal. As a result, the processing of non-personal data is not subject to the obligations imposed on data controllers by the GDPR and its offspring. This is a clear example of how the processes of differentiation within the law precisely aim to identify certain relevant patterns that are made different by other patterns according to how they are matched with their specific normative consequences.[26] This has been, for example, the approach to data regulation across Europe, modelled with the GDPR as the foundation. The GDPR has been constructed around the definition of personal data, but as a result, the related legal regime has also affected that of non-personal data as

[24] Article 1(1) Data Governance Act (n. 21) and Article 2(1) Data Act (Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), COM/2022/68 final).

[25] See n. 21.

[26] Luhmann (n. 12), at 229. Specifically, on the issue of the European integration, see De Witte, 'Variable Geometry and Differentiation as Structural Features of the EU Legal Order', in B. De Witte, A. Ott, and E. Vos (eds), *Between Flexibility and Disintegration. The Trajectory of Differentiation in EU Law* (2017) 9.

the result of differentiation. All that exceeds the definition of personal data included in the GDPR is non-personal data,[27] but quite often data is disruptive with respect to legal definitions.[28]

One problematic issue is that the differentiation of the law is not a single act but a never-ending process, and specifically in the case of GDPR, the attempt at uniformity across Europe has encountered national specificities and legal traditions. It has also created legal frictions in the sense that it is obvious that 'personal data' inherently presents a different relevance in different legal contexts—law enforcement, intelligence sharing, fundamental rights protection. The use of a predefined legal definition risks being based on assumed facts and patterns that continue to change and are constantly differentiated by the law with respect to other social systems. In this sense, Paul De Hert recalls Teubner, arguing that 'Attempts to intervene in subsystems, even with translation, are not necessarily successful because of the resistance of these subsystems to "code" that is not theirs'.[29] This may in particular be the case when it comes machine-learning technologies that are used to process data. This compels the law to be an effective tool for the identification of new legal objects when previous differentiation processes—as in the case of personal/non-personal data—have exhausted some of their effects or are no longer adequate to represent regulatory needs.

Data shapes the boundaries of the law into a variable geometry.[30] At the same time, data is disruptive of any idea of boundaries since its very nature can blur the threshold between what is inside and what is outside the law. Sometimes, however, data moves this threshold across disciplines, territories, policy actions, humans, and machines. It is extremely hard to describe the precise geographical route of data in motion, as data is to be found in many formats and

[27] Article 1 of the Regulation (EU) 2018/1807 on the free flow of non-personal data in the EU, OJ 2018 L 303/59.

[28] One of the thorny points in the separation between personal and non-personal data appears when it comes to pseudonymization and anonymization. Before the GDPR, it was common to see actors (both technical and legal) mentioning pseudonymization as a form of anonymization, and Article 4(5) GDPR seems to be a direct response to this form of dodging, as pointed out by Tosoni, 'Article 4(5). Pseudonymisation', in C. Kuner, L. A. Bygrave, and C. Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 132. Furthermore, anonymization itself is not a stable concept, as what counts as truly anonymized data depends on the risks associated with re-identification in a given moment of time, which are themselves dependent on the technical possibilities for data deanonymization: Almada, Maranhão, and Sartor, 'Article 4 Para. 5. Pseudonymisation', in I. Spiecker gen. Döhmann, *et al.* (eds), *European General Data Protection Regulation* (2022); Finck and Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR', 10 *International Data Privacy Law* (2020) 11.

[29] De Hert, Chapter 4, this volume.

[30] Daskal, 'The Un-territoriality of Data', 125 *Yale Law Journal* (2015) 326; Daskal, 'The Overlapping Web of Data, Territoriality and Sovereignty', in P. S. Bermann (ed.), *The Oxford Handbook of Global Legal Pluralism* (2020) 955.

in many different places. Data is shared across territories and among actors, all beyond specific nation states. In fact, the intangible character of data renders the boundaries of the law more permeable and porous to data flows in various ways. If we consider the physical boundaries of the law, data alters them because it is not based on any territorial linkage with a physical place.[31] Data is also ubiquitous in the sense that it can be used by multiple actors while being accessed everywhere irrespective of where it is located. In the context of interconnected networks, this assumption questions the traditional understanding of the association between sovereignty, jurisdiction, and territory, according to which sovereign powers have jurisdictional claims over a territory.[32] If we instead look at the way in which data reshapes the disciplinary boundaries of the law, data constantly shifts the public–private divide. Governments systematically access private sector data through their cooperation and this creates issues, for example, in terms of reuse of data for purposes other than those initially foreseen at the time of collection. The purpose limitation principle is one of the absolutely core principles of data protection according to which data can be collected for specified, explicit, and legitimate purposes but cannot be processed in a manner that is incompatible with the original purpose for which it was collected. How is that to be implemented in practice when widespread sharing, also by private actors, takes place across territorial limits?

Our contention is that the sharing of data among public actors but also with or by private actors should be regulated by specific agreements, even if this almost inevitably implies that the boundaries of legal categories traditionally belonging to specific areas of the law—such as public law, private law, international law—fade or become fuzzy. Moreover, the interaction of massive data flows with machine-learning techniques inevitably produces hybrid outcomes. Legal rationality quite often struggles to set up its own boundaries with respect to data-driven solutions that are efficient, non-time consuming, and quick to respond. Legal predictions are in fact the result of calculations applied to past data to anticipate probable legal outcomes, as Hildebrandt reminds us time and again,[33] including in her chapter in this book.

The development of AI in the field of public administration offers new opportunities to implement the principle of good administration and the

[31] J. Branch, *The Cartographic State. Maps, Territory, and the Origins of Sovereignty* (2014).

[32] C. Ryngaert, *Jurisdiction in International Law* (2015); Besson, 'Sovereignty', in *Max Planck Encyclopedias of International Law*, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL, (last visited 18 December 2021).

[33] Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics', 68 *University of Toronto Law Journal* (2018) 12.

functioning of public services. This should be coupled with a system of safeguards which ensure the fulfilment of fundamental rights' protection as well as specific requirements regarding the principle of good administration in terms of citizen participation, and transparency and accountability of the adopted AI-based applications. In the area of law enforcement, it is the private sector that remains at the forefront of enforcement. In this respect, automated decision-making appears to have the potential not only to enhance the operational efficiency of law enforcement and criminal justice authorities, but also to undermine fundamental rights affected by criminal procedures. The risk that a shift from post-crime policing to proactive measures based on algorithmic predictions could for instance potentially produce disparate treatment should be carefully addressed. Moreover, predictive crime solutions raise the question of their legitimacy, where AI solutions may affect the right to be presumed innocent until proved guilty.[34]

Law enforcement and policing is obviously not the only field where AI technologies have been successfully applied. AI applications have been widely deployed in different areas of the law, including insurance law, where the calculating capability of algorithms aims to prospectively target probabilities of events and certain individual propensities to experience those events in the future. This field offers relevant examples that come from behavioural policy pricing, customer experience, and coverage personalization, as well as customized claims settlement. The first is based on ubiquitous Internet of Things sensors that provide personalized data to pricing platforms, allowing, for example, safer drivers to pay less for auto insurance (usage-based insurance) and healthier people to pay less for health insurance. The second is based on mechanisms that include chat-boxes pulling on customers' geographic and social data to personalize interactions and customize events and needs (on demand-insurance). The third relies on interfaces and online adjusters that make it easier to settle and pay claims following an accident and decrease the probability of fraud. These examples are emblematic given the risk of discriminatory practices, also in terms of indirect discrimination. Here too, the biased design of AI applications may negatively impact individuals and groups.

In the long run, data-driven solutions may, however, determine convergent solutions regardless of the different surrounding legal cultures and different areas of the law. One of the most relevant examples is the National Security

[34] Mantelero and Vaciago, 'The 'Dark Side' of Big Data: Private and Public Interaction in Social Surveillance, How data collections by private entities affect governmental social control and how the EU reform on data protection responds', 14(6) *Computational Law Review International* (2013) 161.

Agency mass-surveillance scandal that saw different countries systematically violating data privacy using bulk data collection.[35] These examples link to the concerns expressed by the AI Act in different areas. The use of AI systems by law enforcement authorities can be 'characterised by a significant degree of power imbalance and may lead to surveillance'.[36] AI systems used in migration, asylum, and border control management may 'affect people who are often in [a] particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities'.[37] In the field of employment, worker management, and access to self-employment aimed at the recruitment and selection of persons, promotion, termination or task allocation, monitoring or evaluation of persons in work-related contractual relationships, the use of AI 'may appreciably impact future career prospects and livelihoods of these persons'.[38] It is worth noting that the AI Act has identified those practices of AI that shall be prohibited.[39] Among these practices, those that are particularly relevant are those related to AI systems that: deploy 'subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour';[40] exploit any of the vulnerabilities of a social group in order to distort their behaviour;[41] are based on the evaluation of social behaviour (social scoring) or on predictions of personal or personality characteristics aimed at assessing the trustworthiness of individuals, leading to a detrimental or unfavourable treatment;[42] the real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes unless under certain limited conditions.[43] These practices are considered unacceptable because they contravene EU values and fundamental rights.

The levelling functioning of data-driven technologies, if one can call it that, makes it hard to compare the results of specific legal choices as well as those of specific legal institutions and transplants. Legal design alone cannot set up a boundary between law and technology because they are quite radically out of kilter timewise. The time of the law is almost invariably much slower than the time of technology.[44] To be subject to effective regulation, the time of the law

[35] F. Cate and J. Dempsey, *Bulk Collection. Systematic Government Access to Private-Sector Data* (2017).
[36] AI Act, Recital 38.
[37] Ibid. Recital 39.
[38] Ibid. Recital 36.
[39] Ibid. Article 5(1).
[40] Ibid. Article 5(1)(a).
[41] Ibid. Article 5(1)(b).
[42] Ibid. Article 5(1)(c).
[43] Ibid. Article 5(1)(d).
[44] However, this is not always the case, as there are situations in which technology must itself catch up with legal change, for example, when it comes to the adoption of a new legal framework such as the one

and the time of technology as a specific data-driven object of the law should be synchronized in a manner consonant with legal legitimacy. Algorithms make it possible to calculate in advance the compliance of technological performance with the law. For the law it is more complex. Only what is authorized and thus legitimate is allowed although being not necessarily possible, depending upon the personal obedience to legal rules.[45] This difference is irreducible and inevitably creates a temporal gap between the legal and the technological performance that is only addressed by what Lessig ambivalently names the *code*.[46]

The examples discussed above not only address issues of definition but also show how data increasingly pushes the boundaries of the law by creating bridges with changing contexts of relevance. Data is in fact becoming the common currency through which to measure and exchange heterogeneous values, various contexts, and different interests in the sense that it transforms experiences and facts and creates relationships that need to be regulated. This inevitably implies a blurring of possible uses for data flows that also shapes the way in which the law shall face its boundaries. According to a specific legal rationale, a certain use of data may be impeded or allowed by the law and this informs the architecture surrounding the possible consequences. Often, a certain type of data use depends on the available infrastructure and data accessibility. From a linguistic perspective, this means that the law shall increasingly incorporate descriptive tools for defining reality in its own terms, but at the same time the law risks losing its own specificity while enriching its vocabulary.

Data can in and of itself act as a boundary in the sense of constituting an overarching metaphor of the real world: the daily life connections.[47] The law needs to find new strategies to interact with other domains of knowledge, especially when it is not sufficiently clear where information comes from, as is the case with big data. To the extent that the law is capable of incorporating data into legal patterns, it guarantees itself a long life as an autonomous and independent system. Of course, the threshold between autonomy and dependency

provided by the GDPR. While technological artefacts are indeed more malleable than legal institutions, the latter are not inert actors, and the former often take some time to adjust to new circumstances, especially in the case of large-scale systems with many elements that must be updated. For further analysis of the relation between the temporal regimes of law and technology, see Bennett Moses and Zalnieriute, 'Law and Technology in the Dimension of Time', in S. Ranchordás and Y. Roznai (eds), *Time, Law, and Change: An Interdisciplinary Study* (2020).

[45] Hart, *The Concept of Law* (1961).
[46] Lessig, *Code and Other Laws of Cyberspace* (1999), 89–90.
[47] Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era* (2014).

is very narrow and the challenge faced by the law is to ensure its autonomy while being informed and receptive towards the external environment.[48]

3. Digital Borders and Enforcement of the Law

The boundaries of the law—the dividing line between law and non-law—may at some point overlap with the concept of borders—in the sense of the outer edge of the law. This happens in particular when the scope of application of the law is at stake or when the law aims to control the flows of goods and persons. It has been put like this: 'a boundary is not merely a line but a line in a borderland. The borderland may or may not be a barrier'.[49] The main stages in the history of a boundary are the following: the political decision on the allocation of a territory; the delimitation of a boundary in a treaty; the demarcation of the boundary on the ground; the administration of a boundary.[50] The semantic shift from boundaries to borders is also inherent in the foundation of the law.[51] To build itself, the law needs to build its physical limit where one sovereignty ends, and another begins. This represents the core of each sovereign power and requires the exercise of an authority provided by law on a tangible space limited and separated from other spaces. In Carens's words, 'the power to admit or exclude aliens is inherent in sovereignty and essential for any political community'.[52]

Policies on borders are almost always a metaphor of changing times, as we are daily reminded in our newspapers no matter where we are located in the world. It was a clear metaphor during the so-called global war on terrorism and more recently with the refugee crisis, in particular in Europe but also on an ongoing basis in the US. In each crisis, borders come back strongly and play a salient role in making the relevant public authority visible. The EU recently, for example, decided to reopen borders to vaccinated travellers in the form of an app, the Green Pass, thus superseding the temporary reintroduction of internal border control during the pandemic.[53] In the EU, external borders have

[48] Luhmann, *Law as a Social System* (2004).

[49] S. B. Jones, *Boundary Making. A Handbook for Statesmen, Treaty Editors and Boundary Commissioners* (1971) 6.

[50] Ibid. 4.

[51] J. Hagen, *Borders and Boundaries* (2018); Johnson and Post, 'Law and Borders: The Rise of the Law in Cyberspace', 48(5) *Stanford Law Review* (1996) 1367; A. Riccardi and T. Natoli (eds), *Borders, Legal Spaces and Territories in Contemporary International Law* (2019).

[52] Carens, 'Aliens and Citizens. The Case for Open Borders', 49 *Revue of Politics* (1987) 251.

[53] EU Digital Covid Certificate to revive travel in Europe, https://www.etiasvisa.com/etias-news/digital-covid-certificate, (last visited 18 September 2021).

been instrumentalized to enhance security and control, although they do not belong within any notion of European sovereign power as such. Although the external borders are the borders of the countries of the EU and countries that are not members of the EU, the balance struck by the Schengen Agreement on border management has revealed failures. It underlines yet again the age-old fact that the absence of internal border controls for persons in Europe was never coupled with a common policy on asylum, immigration, and external borders.

The boundaries of the law always show their ambivalence on borders. In the case of the EU, this is significant if we consider that the external borders of the EU coincide with the borders of some Member States (for example, Ireland and its border with Northern Ireland, still part of the UK). Strengthening and upgrading the mandates of the EU agencies such as the new Frontex (European Border and Cost Guard Agency), eu-Lisa, European Union Agency for Asylum, and Europol, and also the reinforcement of EU Schengen rules has represented an alternative answer to the lack of internal borders by securing the external borders. The management of external borders, as shared competence provided by Article 77 Treaty on the Functioning of the European Union (TFEU), is in fact the bedrock of a type of composite border management with shared responsibilities. In particular, the administration of borders is the object of multiple forms of delegation from the European Commission and EU agencies in the Area of Freedom, Security and Justice (hereafter: AFSJ).[54]

Recently, AFSJ agencies expanded their operational functions in supporting Member States with new transboundary issues, such as border management, asylum, and migration.[55] The hotspot approach is a clear example of their horizontal cooperation in securing Union standards in the face of the migration crisis. It has also shown how influential AFSJ agencies are in assisting Member States in their national sovereign prerogatives. Examples showing how these agencies determine policies of border administration[56] include Frontex's power to determine the nationality of migrants and its capacity to monitor Member States,[57] Europol's support in the exchange of information

[54] Dehousse, 'The Politics of Delegation in the European Union', in D. Ritleng (ed.), *Independence and Legitimacy in the Institutional System of the European Union* (2016) 57; Hofman, Rowe, and Türk, 'Delegation and the European Union Constitutional Framework', in *Administrative Law and Policy of the European Union* (2011), 222; M. Simoncini, *Administrative Regulation Beyond the Non-Delegation Doctrine: a Study on EU Agencies* (2018), 14, 177.

[55] Nicolosi and Fernandez-Rojo, 'Out of Control? The Case of the European Asylum Support Office', in M. Scholten and A. Brenninkmejer (eds), *Controlling EU Agencies. The Rule of Law in a Multi-jurisdictional Legal Order* (2020) 177.

[56] J. Wagner, *Border Management in Transformation: Transnational Threats and Security Policies of European States* (2021), 209, 227.

[57] Coman-Kund (n. 10), at 163, 167.

and coordination of police operational activities of data extraction related to migrants' transboundary smuggling, and EASO's power to undertake vulnerability assessments in the context of asylum applications. These examples show how flexible the concept of external borders can be and how national authorities can be influenced by EU institutional actors in very sensitive policy areas representing the core of national sovereignty.[58] Indeed, the dynamics of control of the in-between autonomy and interdependence of these agencies, should be carefully considered, taking into account the interaction among multiple executives at national and EU level. It must be borne in mind, after all, that procedural rules should be functional to the tasks that EU agencies pursue and are tied to the interests at stake as well as the inevitable limits.

The Union when imposing these limits must strike a balance between the necessary unity while respecting diversity in the Union.[59] In substantive terms, national authorities are bound to comply with the Union law they implement. This basic tenet of legality follows from the binding nature of Union law underpinned by the principle of supremacy. In procedural terms, national autonomy is limited by primary Union law, including the Charter of Fundamental Rights, Union legislation, and case law of the Union courts. Such limitations are intended to ensure the effective application of Union law but are often the result of precepts of the rule of law as formulated by the Union. But Union law can also impact on the organizational autonomy of national administrations, where, for example, Union legislation requires the independence of national regulatory authorities in the application of Union law. Where representatives of the Member States are integrated within the Union's institutional structure, as is the case of comitology and agencies, they exercise their mandate as part of Union bodies, even though they remain otherwise part of their national organizational structure. This classic dual role may lead to a conflict of interest, but it is an essential aspect of composite administration.[60]

The legal consequences of the integration of national administrations into European administration vary according to the degree of integration in specific policy fields. The national authorities enjoy a certain degree of autonomy when they implement Union law, which is of course limited by the requirements of

[58] D. Fernandez-Rojo, *EU Migration Agencies. The Operation and Cooperation of Frontex, EASO and Europol* (2021) 218.

[59] Article 4(2) TEU.

[60] Schmidt-Aßmann, 'Introduction: European Composite Administration and the role of European Administrative Law', in O. Jansen and B. Schöndorf-Haubold (eds), *The European Composite Administration* (2011); Hofmann and Türk, 'The Development of Integrated Administration in the EU and its Consequences', 13(2) *European Law Journal* (2017) 253; R. Schütze, *From Dual to Cooperative Federalism* (2009).

Union law to ensure uniformity and effectiveness of Union law. This aspect is even more visible in the AFSJ, where the initial intergovernmental origins have included incremental operational and implementation tasks that are not precisely limited by national or EU legal instruments.[61] The case of Europol is illustrative in the way it has engaged in shaping borders through sharing information. The principle of originator control, which requires recipients to obtain the originator's authorization to share data—informs in a tailored way the relationships of Europol with other actors. For example, the European Parliament can be prevented by national authorities from accessing information processed by Europol, resulting in a lack of scrutiny of relevant information.[62] Member States can indicate restrictions on the access and use of information they provide to Europol,[63] and they may have direct access only to certain information stored by Europol.[64] Europol shall further establish its own rules for the protection of classified or non-classified information[65] with obvious implications for originator control (see further Catanzariti and Curtin, Chapter 5, in this volume).

The autonomous data protection framework applying specifically to Europol is also a relevant example of the shared powers that data sharing implies. It shows the tension underlying the model of composite administration in the EU. In fact, the responsibility for the legality of a data transfer lies with: (a) the Member State which provides the personal data to Europol; (b) Europol in the case of personal data provided by it to Member States, third countries, or international organizations (also directly with private persons under the new Commission's amendment proposal). In the context of information sharing, this seems to be far from actual practice. It implies that different layers of administration intertwine with one another also with regard to competences and responsibilities. In terms of data protection obligations, the first controller should be held responsible by virtue of legal status, without a clear distinction of duties. This architecture seems to reflect a double movement increasing formal accountability and at the same time increasing informal autonomy.[66] This relies on a complex interplay between them. Europol's action

[61] Fernandez-Rojo (n. 58) 217.

[62] Article 52 of the Europol Regulation: Regulation (EU) 2016/794, OJ 2016 L 135/53.

[63] Article 19 of the Europol Regulation.

[64] Article 20 of the Europol Regulation. Member States have direct access to information provided for cross-checking to identify connection between information and convicted/suspected persons, and indirect access to information provided for operational analysis.

[65] Article 67 of the Europol Regulation.

[66] Busuioc, Curtin, and Groenler, 'Agency Growth Between Autonomy and Accountability: The European Police Office as a 'Living Institution', 18(6) *Journal of European Public Policy* (2011) 846, at 860.

and its shared competences among different intergovernmental and supranational layers are based on fragmented legal regimes which exist alongside de facto practices of information sharing. The latter plays a crucial role in setting boundaries between competent authorities and expanding or otherwise borders among states.

The amended Europol Regulation weakens the European Data Protection Supervisor (EDPS) supervisory powers.[67] The reform also seeks to enable Europol to register information alerts in the Schengen Information System (SIS).[68] This is arguably paradigmatic of how boundaries of the law and of legal borders may overlap in the field of information sharing.[69] Europol's access to interoperable information systems in the area of security, migration, and external borders management goes in practice far beyond its mandate. The result is that the broader purpose of the so-called integrated border management at external EU borders—which clearly exceeds the mandate of Europol—in practice means control of relevant related information. The proposal for the amendment of the SIS Regulation enabling Europol to enter alerts in the SIS illustrates the trend to increasing the access of Europol to non-law enforcement data[70] and this incremental power of Europol is highlighted in this and related ways in the contribution by Curtin and de Goede in this book (Chapter 6). At the same time, control of information shifts those boundaries of the law that are established between legal areas (law enforcement, intelligence, migration, borders, security), competences, and jurisdictions.[71] Rules on access to data

[67] As put by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ 2022 L 169/1 and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ 2018 L 295/39. See N. Vavoula and V. Mitsilegas, *Strengthening Europol's Mandate. A Legal Assessment of the Commission's Proposal to Amend the Europol Regulation* (2021), 62. On 3 January 2022, the EDPS issued an order to Europol to delete data concerning individuals with no established link to a criminal activity (Data Subject Categorisation), https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (last visited 4 November 2022).

[68] Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, OJ 2022 L 185/1.

[69] See Bossong and Carrapico, 'The Multidimensional Nature and Dynamic Transformation of European Borders and Internal Security', in R. Bossong and H. Carrapico (eds.) *EU Borders and Shifting Internal Security* (2016) 1–21; for an overview on issues related to digital borders and effective protection see E. Brouwer, *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information Systems* (2008), 47 ff., 71 ff.

[70] See the proposed amendments to the Schengen Information System (SIS) regulation: European Commission, Communication COM/2020/791 final.

[71] Jeandesboz, 'Justifying Control: EU Border Security and the Shifting Boundary of Political Arrangement', in R. Bosson and H. Carrapico (eds.) *EU Borders and Shifting Internal Security* (2016) 221–238.

held by Europol and on access by Europol to data provided by third parties are sometimes set up by national authorities, sometimes by Europol, and are often blurred together. This means that information sharing is increasingly becoming a field that includes new paths of shared administration mechanisms but not always effective and adapted accountability mechanisms.[72]

4. Digital Autonomy and European Regulation

Borders are a site for global experimentation using advanced AI technologies.[73] EU initiatives on AI for borders use four categories of AI applications: (1) biometric identification (automated fingerprint and face recognition); (2) emotion detection; (3) algorithmic risk assessment; and (4) AI tools for migration monitoring, analysis, and forecasting.[74] There have been various initiatives on so-called smart borders. These are borders based on the capability to collect and process data and exchange information. The capability of technology to move external borders outside the Union or create digital borders is a way in which the law artificially aligns political and legal boundaries with borders.[75]

In conceptual terms, one might say that data and borders are incompatible, as data is borderless. This means that data, in and of itself, cannot be limited by physical frontiers. Data flows through spaces and across borders, regardless of boundaries of any type. Irrespective of the fact that data evades borders, the law tries to pin it down in various ways. Within the EU, there is a striking and ever-increasing attention to data governance over the course of the past decade. The free circulation of persons and goods has been enabled by data flows in many areas of the law. Conversely, the use of borders as a tool to exercise sovereign powers linked to data can take very different forms. Data enhances the polarity of borders. Although the ubiquitous nature of data that can be accessed and used anywhere makes different spaces replicable or at least closer to each other, at the same time its fragmented character divides, creates frictions, and produces a perception of reality on demand. Data can offer different

[72] See, further, Chapter 6 by Curtin and de Goede in this volume.

[73] M. Longo, *The Politics of Borders: Sovereignty, Security, and the Citizen After 9/11* (2018) 204–228; Akhmetiva and Harris, 'Politics of technology: the use of artificial intelligence by US and Canadian immigration agencies and their impacts on human rights', in E.E. Korkmaz (ed.) *Digital Identity, Virtual Borders and Social Media: A Panacea for Migration Governance?* (2021).

[74] C. Dumbrava, 'Artificial Intelligence at EU Borders: Overview of Applications and Key Issues' (2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRSIDA(2021)690706EN.pdf, (last visited 10 September 2021).

[75] Brkan and Korkmaz, 'Big Data for Whose Sake? Governing Migration Through Artificial Intelligence', 8 *Humanities and Social Science Communications* (2021) 241.

representations of facts depending on how it is aggregated and matched. These facts when filtered through impersonal automated decisions can or cannot be relevant to affect legal or political choices regarding borders. Like all bureaucratic forms based on impersonal law that are applicable regardless of specific situations, algorithms apply indiscriminately and may produce equal results (and possibly related coercive effects) for different personal situations.[76]

Data protection has in fact been used by the EU in order to get around territorial borders. The right to dereferencing (e.g. the removal of links related to personal information) is apparently only for data located within the EU.[77] At the same time, it has also been granted to individuals vis-à-vis companies established outside the EU and against which EU data protection law is applied.[78] With regard to law enforcement access to data more globally, warrants have been issued by public authorities to service providers to release data irrespective of their location storage.[79] As for the global protection of human rights, transatlantic mass-surveillance programmes of individuals have been criticized as being in violation of the right to respect private life under the European Convention of Human Rights.[80] As for the global reach of the European Charter of Fundamental Rights, the Safe Harbor Agreement,[81] and its successor, the Privacy Shield,[82] were declared invalid under EU law for violating Max Schrems' fundamental right to data protection after his data were transferred and physically relocated in the United States.

Data protection law has in fact become an area of the law where the EU has exploited the cross-border potential of data to expand its extraterritorial reach and to limit the interference as well as the impact of other regulatory models in the EU. This has been very clear in the case law of the Court of Justice of the European Union (CJEU), which invalidated international agreements for non-compliance with EU law[83] but also when the Court held that the use of European data by third countries could have implied a violation of EU law.[84]

[76] Visentin, 'Il potere razionale degli algoritmi tra burocrazia e nuovi idealtipi', XX(4) *The Lab's Quarterly* (2018) 47, at 57, 58.

[77] Case C-507/17, *Google LLC, successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL)* (EU:C:2019:772).

[78] Case C-131/12, *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (EU:C:2014:317).

[79] *United States v Microsoft Corp.*, 584 U.S., 138 S. Ct. 1186 (2018).

[80] ECtHR, *Big Brother Watch and Others v the United Kingdom,* Appl. nos. 58170/13, 62322/14 and 24969/15, Grand Chamber Judgment of 25 May 2021.

[81] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (EU:C:2015:650).

[82] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (EU:C:2020:559).

[83] See cases *Schrems I* (n. 81) and *Schrems II* (n 82).

[84] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (EU:C:2014:238), para. 68.

GDPR is a much-quoted example of standard-setting law projecting EU law all over the world, even in countries where the cultural premises of data protection are completely different from those in Europe, such as China,[85] Australia,[86] and Canada.[87] The GDPR embraced a functional approach, seeking to expand EU borders based on individual freedoms and fundamental rights protection and striking a balance with economic liberties. According to this approach, established in Article 3 GDPR, EU data protection law applies in three scenarios: in the context of the activities of a company in the Union regardless of whether the data processing takes place in the Union; upon the offering of goods and services to data subjects in the EU or the monitoring of their behaviour; if the company is not located in the Union, but in a place where domestic law applies by virtue of public international law. In even more explicit terms, the AI Act has a much broader scope than the GDPR, as it basically also applies to providers and users of AI systems that are located in a third country 'where the output produced by the system is used in the Union'.[88] This general formulation considerably expands the scope of EU law all over the world. This tendency shows a specific institutional choice to promote the relevant EU rules all over the world as a model of lawmaking which other countries have to abide with if they wish to enter the European market and more generally have a legal relationship involving data with the EU.

The recent past saw the adoption of elaborate European data protection rules with quite a complex institutional architecture; the present sees the reality of data sharing and the wish to further enhance and regulate such processes. The EU in fact undertook a project to create a strong framework of protection for personal data that focuses on the individual rights of data subjects and ideally should lay down the conditions for the free data flow across sectors, data access, and data reuse for multiple purposes, enhancing business-to-government data sharing in the public interest. In this context of increased demand for data processing in the public and private sectors, recent initiatives have sought to

[85] China's major data protection laws, including the Personal Information Protection Law (PIPL) (effective from November 2021) and the Data Security Law (DSL) (effective from September 2021), are currently in a transitional moment, moving away from a sectorial approach and towards a systemic view of data protection: Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?', 8 *The Penn State Journal of Law & International Affairs* (2020) 49, at 62–84. While this regime differs in some substantial points from the EU data protection regime, notably in the limits to state power, the PIPL provides a comprehensive regulation with some similarities to the GDPR.

[86] For an overview of the differences between Australian and EU data protection systems, see Watts and Casanovas, 'Privacy and Data Protection in Australia: A Critical Overview', *W3C Workshop on Privacy and Linked Data* (2018).

[87] On the Canadian data protection system, see Scassa, 'Data Protection and the Internet: Canada', in D. Moura Vicente and S. de Vasconcelos Casimiro (eds), *Data Protection in the Internet* (2020).

[88] Article 2(c) AI Act.

ensure that the EU can ensure its sovereignty over the conditions of processing of personal data, both in terms of the effective application of the EU data protection framework beyond European borders and, in some cases, of encouraging processing within EU borders.

The EU finds itself now at the crossroads of several different regulatory choices which in general terms can be said to reflect its own digital sovereignty defined in terms of a European take on digital autonomy.[89] The EU aims to avoid digital dependence on third countries but in order to pursue this objective, it identifies and makes recognizable the cultural model it wishes to promote. This model is basically grounded on data protection, trustworthy standards for data sharing of privately held data by other companies and governments, and of public sector data by businesses.[90] At the same time, data has reinforced the desire for sovereignty of the EU, on the assumption that by linking sovereignty to its 'digital' vision it can consolidate its existing position. By contrast, justifying it legally would have been hard, as the term 'sovereignty' never appears in the Treaty on European Union (TEU) or in the TFEU.[91] In reality, the capacity of Europe to manage huge flows of data is greatly limited by foreign digital infrastructures. The latter's operational rules in fact determine the effective power of the EU to control data flows. The real challenge for Europe is to avoid undue dependence on foreign digital infrastructures. As pointed out by Celeste 'the main rationale behind digital sovereignty claims in the EU lies in the desire to preserve European core values, rights and principles' while exerting full control over data including storage, processing, and access.[92] This is part of a broader phenomenon mostly triggered by data protection law, as also observed by De Hert in Chapter 4. He points to how European data protection, as an EU policy area, is not an independent goal in itself, but is to be seen as part of larger agenda of the Digital Single Market, a strategy aiming to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy.

[89] L. O'Dowd, J. Anderson, and T. W. Wilson, *New Borders for a Changing Europe. Cross-Border Cooperation and Governance* (2003).

[90] European Commission, 'A European Strategy for Data', COM/2020/66 final.

[91] Christakis, *European Digital Sovereignty. Successfully Navigating Between the 'Brussels Effect' and Europe's quest for Strategic Autonomy*, https://cesice.univ-grenoble-alpes.fr/actualites/2020-12-15/european-digital-sovereignty-successfully-navigating-between-brussels-effect-and-europe-s-quest, 8, (last visited 16 July 2021). See also Avbelj, 'A Sovereign Europe as a Future of Sovereignty?', 5(1) *European Papers* (2020) 299.

[92] Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives', in F. Fabbrini, E. Celeste, and J. Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (2021) 211.

In seeking digital autonomy, the EU aims to avoid resorting to protectionist practices of data governance in a sort of imitation game. After all cross-border data control practices determine the risk of retaliation by other states.[93] For example, the adoption of the CLOUD Act (Clarifying Lawful Overseas Use of Data Act) in the US—an Act that enables public authorities to compel private intermediaries to hand over data regardless its location, even outside the US—might be read as a reaction to European activism towards the expansion of the scope of the European Charter of Fundamental Rights and the GDPR beyond the Atlantic.[94] It created a conflict of jurisdiction with the GDPR since US requests for data located in Europe that are lawful under US law cannot now be blocked. Understanding this process under the lenses of the law and its boundaries sheds light on the steps needed to lead to an autonomous data infrastructure compatible with EU regulatory trends. It is also a good example of how physical borders matter in an interconnected world, notwithstanding the original optimism regarding the role of the internet.

5. A New Regulatory Compass for the EU

A digital single market of data flowing across and through the EU aims to ensure technical competitiveness and the autonomy of relevant infrastructures. To develop this goal, fundamental rights and property rights need protection but at the same time trust among actors who share data also needs to be built. The ambition is to create a framework in which the principles enshrined in data protection law can be reconciled with the interests of individuals and businesses to access digital goods and services and maximize the growth potential of the digital economy. The new model of the European data strategy is based on a set of legal instruments with twin aims. First, to improve specific regulatory segments for online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms in order to develop a single market for data, avoiding platforms as gatekeepers to the internal market (Digital Services Act and Digital Markets Act). Second, to make public sector data available for reuse in situations in which this data is subject to the rights of others, such as personal data, data protected by intellectual property rights, or data that contains trade secrets or other commercially sensitive information (Digital Governance Act, hereinafter 'DGA'). This ambitious

[93] Ibid. 61.
[94] See cases *Schrems I* (n. 81), *Schrems II* (n.82), and *Digital Rights Ireland* (n.84).

initiative is intended to enhance access to data for individuals, businesses, and administrations. It takes for granted the *acquis* of the GDPR as a building block upon which a new set of regulatory tools can be built, regardless of any possible misalignments.[95] Once data is protected, the idea is that it should also be managed during its whole lifecycle. The EU has bet on a model of data management based on the 'recycling' by private entities of data initially stored by public authorities. In particular, the DGA has four main pillars: (1) making public sector data available for reuse; (2) sharing of data among businesses, against remuneration in any form; (3) allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the GDPR; (4) allowing data use on altruistic grounds. This regulatory instrument seeks to overcome the public–private divide providing a cooperative framework between private- and public-sector data that is supplied as part of the execution of public tasks, with the exception of data protected for reasons of national security.

The AI Act functions as a type of *passe-partout* crosscutting these various new regulatory strands and aims to address critical issues of the data-driven market. It provides a further body of rules, formulated under the legal basis of Article 114 TFEU, to ensure the establishment and the promotion of the internal market and, specifically, of lawful, safe, and the trustworthy use of AI systems. Data represents the drive of a broad legislative process that aims to provide a consistent legal toolkit to address the challenges of the blurring of many existing boundaries between data and the law: which data can be shared, which data can be used by AI systems, which data needs specific safeguards. Data control is in fact the most effective way to enhance security, both at a substantive level and at the technical organizational level. Several regulatory instruments have recently tried to implement the multifaceted goal of security in different regulatory segments: protection of networks and information systems; interoperability of information systems in the field of police and judicial cooperation, asylum, migration, visa, and borders; processing of special categories of data by police (biometric verification and identification); European integrated border control. In the field of security management, information sharing is of particular relevance in the context of mechanisms of composite administration. However, it is never clear, particularly in the field of law enforcement, whether personal data belongs to data subjects or authorities, be they domestic, European, or foreign. Moreover, when personal data

[95] The compatibility of definitions like 'data holder' in the DGA and 'data user' in the GDPR is not clear, nor is the distinction between data belonging to physical persons or legal persons.

processing is enhanced by the use of AI systems, it is not always easy to put a clear line of demarcation between law enforcement purposes, on the one hand, and border management, asylum, and migration purposes, on the other hand.[96] For example, the AI Act does not generally allow the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless specific conditions are met,[97] but it broadly applies to AI systems used for border control management, migration, and asylum.[98] In practice, the boundary between law enforcement and migration, borders, and asylum is not clear enough.[99] The new institutional framework of interoperable information systems in effect overturns the purpose limitation principle, one of the boundaries of data protection law, according to which data should be processed only for specified, explicit, and legitimate purposes and

[96] Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues', 8 *Journal of National Security Law & Policy* (2016) 473.

[97] Article 5 1(d) and Recital 38 AI Act.

[98] Pursuant to Recital 39 AI Act (n. 37), these systems are for example polygraphs and similar tools or to detect the emotional state of a natural person or those intended to be used for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status.

[99] Annex III of AI Act specifies that both law enforcement and migration, border and asylum are high-risk AI systems and differentiates them as follows: Law enforcement AI systems includes (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences; (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person; (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in Article 52(3); (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences; (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences; (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data. Migration, asylum and border control management AI systems include (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person; (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State; (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features; (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

not for further purposes incompatible with the original ones.[100] Although the law constantly sets up boundaries among the activities that fall (or do not fall) within its specific field of application, the ability of data to blur these boundaries is magnified by the way technologies make it possible to use data.

Finally, international negotiations on cross-border access to electronic evidence, necessary to track down dangerous criminals and terrorists, are currently ongoing, and the proposal on e-evidence is at the final stage of public consultation.[101] It is significant that in the field of law enforcement, the Law Enforcement Directive does not allow—unlike the GDPR—the recognition of any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data to be recognized or enforceable in any manner. This is irrespective of whether or not it is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. This illustrates how physical boundaries among the EU and third countries are resistant to data processing for law enforcement purposes that imply exchange of information among third countries. Law enforcement data sharing often happens at an informal level which is quite often at the boundaries of the law.[102]

6. Data-Driven Law as Performance and Practice: European Intermezzos

As has been recalled many times, the GDPR can still be considered a type of modern-day foundation stone that spawned, or has been mimicked in, various other regulations.[103] The GDPR has seen a growth in practice (and eventually

[100] Article 5 GDPR. See Vavoula, 'Databases for Non-EU nationals and the Right to Private Life: Towards a System of Generalized Surveillance of Movement?', in F. Bignami (ed.), *EU Law in Populist Times: Crises and Prospects* (2020) 227, at 227–266, 231–232; Brouwer, 'A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime', *Un-Owned Personal Data Blog Forum*, https://migrationpolicycentre.eu/point-no-return-migration-and-crime/, (last visited 10 September 2021); Bunyan, 'The point of no return', *Statewatch Analysis* (updated July 2018), https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf, (last visited 10 September 2021).

[101] European Commission, *E-evidence — cross-border access to electronic evidence* (2021), https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidenceen (last visited 17 December 2021).

[102] Aguinaldo and De Hert, 'European Law Enforcement and EU Data Companies: A Decade of Cooperation Free from Law', in E. Celeste, F. Fabbrini, and J. Quinn, *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (2020) 157; Daskal, 'The Opening Salvo. The CLOUD Act, the e-evidence Proposals, the EU-US Discussions Regarding Law Enforcement Access to Data Across Borders', in F. Bignami (ed.), *EU Law in Populist Times* (2020) 319.

[103] See De Hert, Chapter 4, this volume.

also in regulation) alongside it, bordering it as it were, in particular in the field of law enforcement and (national) security.[104] The thrust of the book is deliberately not Eurocentric but rather aims to give voice to scholars based in Europe to reflect on problems of principle in terms of law and its boundaries as relating to data systems in their various aspects. This is at times Europe focused if the object is an evaluation of regulatory instruments, which some consider potentially world leading, and at times the object is a much broader and more general remit. What is arguably distinctive about this collection of chapters by a number of leading legal scholars—and one political scientist—in Europe is that its focus is not on the GDPR when it comes to data and issues of access, use, and sharing (as opposed to processing). Rather the focus across all chapters is on data access, use, and sharing essentially by public authorities (although private actors inevitably intersect with this). It is also on the institutional choices that make Europe an international actor and a competitive interlocutor in the area of data-driven governance. Given that the backdrop is data and that the market on data is global with so many data providers or data intermediaries located outside Europe and also subject to other jurisdictions in law and otherwise, this book covers both more general issues on which there are substantial theoretical and legal debates globally[105] as well as more specific issues that either are already grounded in specific EU regulations[106]—or may well be.

A more specifically European take on more general issues is of value and we hope will contribute to various ongoing debates around the globe and be of interest not only to scholars, lawyers, and political scientists who study data-driven processes but also those working on the meaning and substance of much broader issues in the modern world, such as transparency, accountability, the role of public authorities, and territorial issues that go beyond borders and jurisdictional questions. The other way in which the authors of this volume give a European perspective is by not only all being European, employed at European universities but, more importantly, even when speaking to general theoretical or wider conceptual themes, we all use European examples where appropriate.

Mireille Hildebrandt in Chapter 2, which opens the collection after this introductory chapter, reasons at a general level on the boundaries between text-driven modern law and computational law with specific attention to the case of legal judgments and machine learning technologies to predict legal judgments.

[104] See Curtin and de Goede, Chapter 6, as well as Catanzariti and Curtin, Chapter 5, this volume.

[105] See for example the Compulaw Project. Governance of Computational Entities Through an Integrated Legal and Technical Framework (ERC Advanced Grant), https://site.unibo.it/compulaw/en, last visited on 11 February 2022.

[106] De Hert, Chapter 4, this volume.

She conducts boundary work between modern positive law and technological determinism. She explores the differences between the *performativity* of legal norms (based on positivity, multi-interpretability, and contestability) and the *performance* of predictive legal technologies, arguing that the latter is disruptive of the way of existence of the law 'as we know it': 'If legal practice were to adopt these kinds of technologies, it may end up disrespecting the boundary between a law that addresses people as human agents and a law that treats them as subject to a statistical, machinic logic.' Hildebrandt argues that the 'affordances' of data-driven modern law cannot be integrally transposed into the use of predictions as a new way to establish the law, because human anticipation and machine anticipation are profoundly different. Text-driven anticipation has a qualitative probability that relies on 'doing things with words'. It is constituted by the performative effect while data-driven prediction, based on mathematical assumptions, has a quantitative probability and its effect is caused by the fulfilment of the conditions. Turning legal anticipation into data-driven prediction has a clear impact in terms of effects on legal protection 'that is *part of* law's instrumentality', in the sense that it allows individuals to 'contest claims of validity regarding both legal norms and legally relevant facts'. Legal protection by design and legality by design are not equivalent, but the gap between the two can be filled by human oversight, as now provided by the terms of the draft AI Regulation.

This is certainly also the case for understanding transparency more conceptually as it relates to automated practices. In Chapter 3, Ida Koivisto digs deeply into the value of transparency as well as some aspects of its conceptualization in the digital context. She questions whether the promise of transparency in the GDPR is in fact a normative rationale, or only an umbrella concept or a more general interpretative concept. She argues that the line between secrecy of automated processes and transparency is very thin, especially when it is not clear what the principle of transparency should protect: readability of data, explanation of processes, or fair procedures. Koivisto correctly warns about the tautology of transparency, which is 'performative in nature' and may turn to a simplistic meaning of being able to see a transparent object, the inner functioning of machines, and not instead a 'meaningful information of the logic involved'. This means that transparency is performative as far as it makes visible only a transparent object that can be seen and into which we can see inside, but it keeps secret what lies behind it. She perceptively notes that 'seeing inside the black box does not necessarily lead to understanding, and understanding does not necessarily lead to control or other type of action'. Therefore, explainability seems to be the most

accountable declination of the principle of transparency, understood as 'description of logics to justification'.

Moving to the more specific phenomenon of GDPR mimesis, according to Paul De Hert in Chapter 4, this is present in various EU legislative instruments, in particular the Network and Information Security Directive, the EU regulations on drones,[107] and the DGA as well as the AI Act. He argues that the GDPR has formulated a type of EU model for technology regulation, a kind of *acquis*, but without an adequate or full integration of the principles enshrined in the GDPR. Among the factors that have increased mimesis among different measures are the institutional tendencies to adopt very general measures—what De Hert calls 'open texture' and EU-wide agencification. These factors are exemplified by general rules often included into regulations seeking to harmonize national laws and ex post uniformized by legally binding decision of the Luxembourg Court or in case of political disagreement by the action of EU agencies, that act as 'epistemic communities … with shared knowledge, culture, and values'. Arguably, lack of creative legal thinking by those drafting legislation as well as path dependency with previous legislative choices and the coexistence of regulatory spaces have played a crucial role in the repeated spread of the norms of the GDPR without looking to the bigger picture of what these repeated steps means in terms of overall EU integration.

An example of the lack of integration of the GDPR in other contexts of data processing that are not represented by a few distinct legislative measures is the interoperability of information systems used for migration, asylum, and borders. The analysis of data originalism conducted by Mariavittoria Catanzariti and Deirdre Curtin arguably offers a new conceptualization of personal data sharing. It reflects upon the original status of data—personal and thus non-appropriable by any authority or individuals—but also on the role of data originators, namely those authorities who originate data and share them first. The authors argue that although originators can set up specific rules for data sharing, the original status of personal data as non-appropriable entities is not to be undermined. This in practical terms implies attaching broad data protection safeguards plus specific rules set up by data originators for data sharing among users that have access to interoperable data. It is an odyssey in many ways to untangle and deconstruct interoperability not only conceptually but

[107] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ 2016 L 194/1; Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ 2019 L 152/45; and Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ 2019 L 152/1.

also in terms of its possible legal neighbours and peers. The authors believe that such detailed analysis is not only essential in and of itself for a better conceptual and legal understanding but also in the process reveals the political lurking in the shadows.

A final contribution by Deirdre Curtin and Marieke de Goede explores the byzantine complexity of what is now known generically as interoperability, which breathes technical configurations and exchanges rather than legal analysis and its positioning in accountability terms. The authors reveal how data-led security, represented by policies and practices of security integration through the building and connecting of databases, is a concept that involves a cross-border dimension but also different levels of decision making. Both of these factors are reflected in different and multiple purposes of data processing that are hardly integrated at all. To approach the boundaries of what we know (and do not know) through data, this chapter investigates the role of accountability in a data-driven security explored throughout various case studies, such as tracking terrorist financing, targeting terrorist online content, and interoperability. In the opinion of the authors, data-led security should be coupled with mechanisms of logged-in accountability that prevent *ad hoc* or in any event limited forms of oversight. The practice of 'logging' is then inspected through the scrutiny of the adequacy or inadequacy of its standardized format that often leaves accountability mechanisms simply not connected to the actual data analysis in practice.

The common thread of these six chapters is the intrinsic tension between the transformations taking place as a result of data flows affecting individuals, institutions, legal regimes, and practices, and the reality of the bounded nature of the law when faced with the use and sharing of data. The responses have tackled specific areas of relevance where they criss-cross key issues of democratic legitimacy, the process of European integration, and the evolving digital European strategy. Our aim as editors has been to raise the wider issues and to make a contribution to the more global debate on the basis of a more granular and sectoral understanding of the way that European law and institutional practice is taking shape and maybe occasionally leading in terms of specific choices that are being made. Our purpose is certainly not to push a 'Brussels effect' or its equivalent, but rather to dig deeper into the lesser-known areas of data that can, for one reason or another, be said to be at the boundary or borders of law. The 'intermezzos' in this book are however part of a much wider performance that takes place and is influenced globally and not only in Europe.