Comparative Legal Metrics - Symposium

The Power of Numbers and the Role of Law: On the Way to the Global Accountability of Transnational Actors?

Giorgio Resta*

Abstract

The quantification of performance has everywhere become a tool of governance, an instrument capable of influencing the behaviour of individuals and other entities, and thus a potent source of power. How does (or should) the law regulate the exercise of such power? This paper addresses this question by providing a comparative overview of recent regulatory trends. In particular, it sheds light on the thorny issue of how to ensure the accountability of transnational actors and reflects on the controversial trend towards extraterritoriality, which is well illustrated by recent EU digital regulation.

I. Legal Metrics in Comparative Law

The book, edited by Mauro Bussani, Sabino Cassese, and Marta Infantino is an invaluable contribution to a better understanding of one of the most significant phenomena shaping our societies, and namely governance by numbers.[1] Of course, this is not the first volume to deal with this topic,[2] and the editors themselves have previously written other pioneering essays and monographs focusing on indicators and quantitative methods.[3] However, 'Comparative Legal Metrics' has two features, both reflected in its title, that distinguish it from the existing literature.

First, it has a broad geographical scope, taking into account the experiences of different societies from different parts of the world. However, it is not simply a description of such experiences as isolated entities. It makes use of comparative law methodologies to provide – particularly in the first and the last chapters –

* Full Professor of Comparative Law, Roma Tre University.

[1] M. Bussani et al eds, *Comparative Legal Metrics: Quantification of Performances as Regulatory Technique* (Leiden-Boston: Brill, 2023).

[2] One might simply recall A. Supiot, *La gouvernance par les nombres: Cours au Collège de France (2012-2014)* (Paris: Fayard, 2015).

[3] See only M. Infantino, *Numera et impera: Gli indicatori giuridici globali e il diritto comparato* (Milano: FrancoAngeli, 2019); Id, 'Global Indicators', in S. Cassese ed, *Research Handbook on Global Administrative Law* (Cheltenham: Edward Elgar, 2017), 347-367; S. Cassese and L. Casini, 'The Regulation of Global Indicators', in K.E. Davis et al eds, *Governance by Indicators: Global Power through Quantification and Rankings* (Oxford: Oxford University Press,2012), 465-474; M. Bussani, 'Credit Rating Agencies' Accountability: Short Notes on a Global Issue' 10 *Global Jurist*, 1 (2010).

both an in-depth analysis of local conditions and a careful assessment of differences and similarities, as well as a generalization of the findings of each national or regional report. Following the path of a consolidated tradition, it crosses not only the jurisdictional boundaries, but also disciplinary boundaries, and namely the public law/private law divide, which is meaningless in transnational settings.[4] It is therefore a comparative law book in the fullest sense of the notion.

Second, it focusses on different typologies of quantification of performance in various sectors (mainly justice, education, and market-related activities), which have in common the attitude to produce 'legal effects'. Such a notion is to be understood flexibly, beyond any formalistic assumption about what constitutes law in a particular jurisdiction. From a realist and pluralist point of view, it could include any factor that could significantly and regularly influence social behaviours. As the editors make clear in the introduction, the adjective 'legal' refers to the

> 'direct or indirect regulatory effects that the act of measurement has on the behavior of the subjects involved in the measurement process, including not only the measured, but also the measurers and those who rely on the measurements'.[5]

By looking at different societies (representing several legal traditions and political systems) and by adopting a rigorous analytical framework, the book provides a comprehensive analysis of some of the most important questions raised by of 'governance by numbers'.

These include: a) in which areas is quantification of performance most common? *b*) who are the relevant actors? *c*) who is affected? *d*) what are the main typologies of legal metrics? *e)* why has regulation by numbers become so widespread? *f)* how should legal metrics be regulated?

II. The Power of Numbers and the New Sovereigns

Chapters from 2 to 15 deal with questions from *a)* to *e)* and explore the complex morphology of legal metrics in different sectors and legal systems.

Reading these contributions, one gets the impression that quantification of performance has everywhere become a tool of governance, an instrument capable of influencing the behavior of individuals and other entities, and thus an important source of power. A power that is more insidious than the classic Weberian ideal type that underlies the traditional legal approach to the problem of authority.[6] This has essentially been limited to situations where there is a

[4] See M. Bussani et al, 'Quantification of Performance as a Regulatory Technique: A Comparative Appraisal', in Ead eds, *Comparative Legal Metrics* n 1 above, 332, fn 37.

[5] ibid 3-4.

[6] See M. Renner, 'Machtbegriffe zwischen Privatrecht und Gesellschaftstheorie', in F. Möslein ed, *Private Macht* (Tübingen: Mohr Siebeck, 2016), 505 et seq.

subject who is in a formally recognized position of supremacy, and who as such is able to impose her own will on the legal sphere of others. Paradigmatic is the relationship between the public administration and the citizens, but also in private law some exceptional forms of 'private powers' were quite early recognized, and among them the position of the employer, *vis-à-vis* the employees, and the husband, *vis-à-vis* other members of the family. Relationalism, the vertical dimension, coercion, and transparency are thus the features that characterize the 'traditional' legal conception of power and shape the remedies devised to protect the passive subject.[7]

Here, by contrast, we are faced with a power that is granular and fundamentally acephalous, opaque and often incomprehensible, persuasive rather than coercive, manifested in the dimension of fact rather than that of (formal) law, and is located in spaces that do not coincide with the physical locations of the nation-state. It is therefore the prototype of the 'new powers',[8] which fit better into a Foucauldian rather than a Weberian theoretical framework. Power relations, according to the French philosopher, are no longer placed in a linear register that identifies an active subject, generally consisting of the state and its articulations, a passive subject and a typical effect in the sense of conditioning the will through coercive or prohibitive acts.[9] From this perspective, power is not necessarily coercive, since it is itself a condition of the thinkability of the world, orienting forms of knowledge, selecting themes and patterns of argumentation. It cannot therefore be understood on the basis of what Foucault calls the juridical conception of power, characterized by a logic of command that generates resistance. It expresses itself in a plurality of places and in forms other than those typically repressive.[10] The new, Foucauldian power has a generative force that cannot be underestimated; in its most incisive and least volatile expressions

> 'it doesn't only weigh on us as a force that says no, but that it traverses and produces things, it induces pleasure, forms knowledge, produces discourse. It needs to be considered as a productive network which runs through the whole social body, much more than as a negative instance whose function is repression'.[11]

This perfectly explains the 'magic of numbers' explored in this book.
The quantification of performance is cloaked in the aura of voluntariness,

[7] See for a detailed analysis G. Resta, 'Poteri privati e regolazione', in M. Cartabia and M. Ruotolo eds, *Enciclopedia del diritto: Potere e Costituzione* (Milano: Giuffrè, 2023), 1008.

[8] M.R. Ferrarese, *Poteri nuovi: Privati, penetranti, opachi* (Bologna: il Mulino, 2022), 140.

[9] P. Franzosi, 'A Reflection on Power and Knowledge in Michel Foucault' 77 *The Political*, 135, 143 (2012).

[10] G. Turkel, 'Michel Foucault: Law, Power, and Knowledge' 17 *Journal of Law & Society*, 170 (1990).

[11] M. Foucault, 'Truth and Power', in Id ed, *Power/Knowledge: Selected Interviews and Other Writings (1972-1977)* (New York: Vintage, 1980), 119.

rationality, intelligibility. As such, it is not perceived as a force that says no, and triggers resistance, but it 'traverses and produces things (…) forms knowledge, produces discourse'.[12] It is also productive in the sense that it influences behaviours in the direction desired by those in power.

We all know – and the authors of this book rightly remind us – how the rankings work: Countries reform the regime of security interests not always because they think it is necessary, but because it helps to achieve better positions in the World Bank Doing Business Report;[13] universities strive to attract more and more international students not necessarily because the management thinks that diversity in the classes ensures a better environment for teaching and learning, but because it helps to climb the QS or THE rankings; the main concern of professors is to publish (even to the detriment of other relevant activities such as studying?), and to publish in certain series or reviews, because the allocation of funds or even the recruitment is directly or indirectly based on numerical indicators;[14] market players offer certain products or services (or stop offering certain products or services) because otherwise they could incur in a negative evaluation by the customers, which could put them out of business.

Despite the absence of a vertical relationship and a formal assertion of authority, individuals and other legal subjects are caught in a framework characterized by the exercise of a subtle, opaque, but highly effective form of power that is difficult to resist, if not for other reasons because it is not perceived as such.[15]

III. What Regulation?

Since no well-ordered society can tolerate unchecked powers, the challenge for our legal systems is how to make these new forms of power accountable. This is not an easy task, from any point of view. Bussani, Cassese, and Infantino deal specifically with this issue in the last chapter of the book.[16]

They distinguish two main situations, depending on whether a possible regulation targets domestic actors or transnational entities.

Domestic regulation is proliferating in both the public and private sectors. As several examples in the book show,[17] they can take the form of prohibitions (as in the case of Art 5 of the EU AI Act), risk management mechanisms, procedural

[12] ibid

[13] See M. Infantino, n 3 above, 145 et seq.

[14] See A. Jakubowski, 'Quantification and Parameterization of Legal Research: The Case of Poland', in M. Bussani et al eds, *Comparative Legal Metrics* n 1 above,118.

[15] See M. Bussani et al, 'A Comparative Appraisal' n 4 above, 354-358.

[16] ibid 358-362.

[17] See for instance I. Cardillo, 'Governance and Quantification of Performance in China', in M. Bussani et al eds, *Comparative Legal Metrics* n 1 above, 180 et seq; R. Gottardo, 'Algorithmic Decision-Making and Public Sector Accountability in Africa – New Challenges for Law and Policy', in M. Bussani et al eds, *Comparative Legal Metrics* n 1 above, 139.

techniques, the granting of individual rights and remedies (as in Arts 15 and 22 GDPR). However, their effectiveness remains to be seen, especially in the light of technological developments that make it extremely difficult to understand the most sophisticated systems of quantitative assessment. Looking at the latest generation of artificial intelligence (AI) systems, which are often used to analyze a wide range of data, infer consequences, and draw up rankings, there is maximum opacity both in terms of the type of data used to train the algorithms and the logic followed by the machine to reach a conclusion.[18]

Unlike early automated systems, today's AI tools are based on learning by doing, making it difficult even for skilled programmers to understand why and how a particular result was achieved.[19] As a consequence, any person affected by AI systems will find it hard to understand the logic behind a particular decision (eg the marks awarded), to present counterarguments, and, ultimately, to challenge it in court.[20] Moreover, the normative framework of intellectual property rights indirectly reinforces such technological enclosure, making opacity by design an institutional feature of the system. In particular, trade secrets and copyright are often interpreted so broadly that the information needed to understand the logic behind such decisions (and to have them reviewed) is simply not available.[21] The famous Loomis case,[22] as well as recital 63 Regulation 2016/679 (GDPR)[23] clearly illustrate this point.

When it comes to transnational actors (including international organizations, multinational corporations, NGOs, digital platforms), regulation is even more difficult. As the authors put it,

> 'the current absence of any call for an international treaty on the field, and considering the general regulatory and jurisdictional immunity enjoyed by actors in the international arena, it seems that performance-based measures produced by international organizations and alike are bound by no rule other

[18] See S. Grumbach et al, 'Autonomous Intelligent Systems: From Illusion of Control to Inescapable Delusion', available at https://tinyurl.com/3xnuc5xa (last visited 30 September 2024).

[19] J.A. Kroll, 'The Fallacy of Inscrutability' 376 *Philosophical Transactions of the Royal Society A*, 1 (2018); H. Shah, 'Algoritmic Accountability' ibid.

[20] D. Keats Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' 89 *Washington Law Review*, 1 (2014).

[21] D. Levine, 'Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure' 59 *Florida Law Review*, 135 (2007).

[22] *State* v *Loomis* 881 N.W.2d 749 (2016).

[23] 'A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing (…) Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. (…) That right *should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software*'.

than self-made ones'.[24]

According to the editors, the theory of global administrative law could provide a possible way out.[25] In particular, they argue that global administrative standards, such as transparency and accountability, could be particularly useful. Indeed, despite the absence of a formal system of enforceability, they are often complied with spontaneously by transnational actors, pressured by 'expectations and demands by interested parties and by the public'.[26]

This is a profound observation, in line with the gradual erosion of territory as the main criterion for justifying jurisdictional claims. The law of the cyberspace and more generally the regulation of digital technologies offers a privileged perspective from this point of view, which is particularly relevant for the type of issues discussed throughout the book.

The quantification of performance, at least in its most sophisticated forms, is hardly conceivable without recourse to a wide gamut of data and AI tools.[27] Consider, for example, a digital lending platform (like SoFi) that wants to rate its customers, a government (like Australia) that wants to select prospective immigrants based on a sophisticated scoring system,[28] or an employer (like Uber) that wants to algorithmically assess the performance of many employees.[29] Such decisions typically involve the collection of a significant amount of personal data, the processing of that data, the use of AI tools to build profiles and the ranking of relevant individuals according to pre-defined criteria.

The fact that we live in an interconnected world, makes it extremely common for such activities to take place across jurisdictional boundaries. Data is produced or collected in country X, simultaneously stored in servers located in countries Y, Z, instantaneously moved from one place to another, broken up into packets and routed through nodes that may be located in multiple jurisdictions.[30]AI models designed in country A and launched in country B, are deployed in country C.[31] Customers in countries X, Y and Z are evaluated by the company based in country W. The data and AI value chain has become so fragmented that one of the biggest challenges facing our legal systems is how to ensure accountability in an increasingly complex transnational environment.

[24] See M. Bussani et al, 'A Comparative Appraisal' n 4 above, 358.

[25] S. Cassese, 'Administrative Law Without the State? The Challenge of Global Regulation' 37 *New York University Journal of International Law and Politics*, 663 (2005); Id, *An Advanced Introduction to Global Administrative Law* (Cheltenham: Edward Elgar,2021).

[26] ibid

[27] See M. Bussani et al, 'An Introduction' n 5 above, 14.

[28] For some examples M. Tani, 'Using a Points System for Selecting Immigrants' 16 *ifo DICE Report*, 8 (2018).

[29] For some examples M. Hu, 'Algorithmic Jim Crow'86 *Fordham Law Review*,633 (2017).

[30] J. Daskal, 'The Un-Territoriality of Data'125 *Yale Law Journal*,326 (2015).

[31] See for instance M. Senftleben, 'AI Act and Author Remuneration – A Model for Other Regions?' available at https://tinyurl.com/4nwt9czc (last visited 30 September 2024).

We have gone through different models and approaches.

In the beginning, the logic of jurisdictional self-restraint was embedded in the libertarian idea of the Internet as a de-territorialized domain, shielded from the influence of traditional sovereigns. This was the era of unfettered freedom for providers to host content uploaded by third parties without fear of liability, of anonymity of communications as a dogma, of data localization requirements as a taboo.[32] Traumatic events such as the NSA and the Cambridge Analytica scandals suddenly revealed a different reality: the physical and electronic space previously thought to be a-territorial was in fact the object of a peculiar form of public-private colonialism; the power exercised by the digital oligopolies proved to be symbiotic with the public authority of a certain Western government and its closest allies;[33] the theoretical choice against territoriality went hand in hand with the factual assertion of extraterritorial jurisdiction through the market dominance of United States (US) -based corporations.[34]

As a result, different models gained traction.

China had initially rejected the open texture of the Western digital globalization by adopting an opposite strategy, which was reflected into the Great Firewall, the extensive data localization requirements, the strict controls on content posted online, and a ban on anonymity.[35] China was followed by Russia and other countries, occasionally influenced by the Digital Silk Road Initiative.[36]

Even the European Union (EU) has gradually tightened up its open system of digital governance. Formerly a paladin of the free flow of data and of technological neutrality, nowadays the EU now seems to have taken the opposite path, influenced by ideas of technological independence, proactive assertion of digital sovereignty, and increasing recourse to the territorial extension of EU law.[37] In particular,

[32] See generally A. Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 33 et seq; J.E. Cohen, *Between Truth and Power: The Legal Construction of Informational Capitalism* (Oxford: Oxford University Press, 2019).

[33] On the NSA scandal see C. Bowden, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights* (Lëtzebuerg: EUR-OP, 2013).

[34] A. Chander and H. Sun, 'Introduction: Sovereignty 2.0', in Ead eds, *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford: Oxford University Press, 2023), 16.

[35] Y. Wang, 'Regulating Outbound Data Transfer: The Practice of China and a Comparative Approach', in M. Timoteo et al eds, *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China* (Cham: Springer, 2023), 169-180; A. Chander and H. Sun, 'Introduction' n 34 above, 8; H. Gao, 'Data Sovereignty and Trade Agreements: Three Digital Kingdoms', in A. Chander and H. Sun eds, *Data Sovereignty* n 34 above, 225 et seq.

[36] A. Chander and H. Sun, 'Introduction' n 34 above, 14 et seq; G. Greenleaf, 'Personal Data Localization and Sovereignty Along Asia's New Silk Roads', in A. Chander and H. Sun eds, *Data Sovereignty* n 34 above, 295.

[37] A. Bradford, *Digital Empires* n 32 above, 134 et seq; T. Christakis, 'European Digital Sovereignty, Data Protection, and the Push toward Data Localization', in A. Chander and H. Sun eds, *Data Sovereignty* n 34 above, 371; E. Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives', in F. Fabbrini et al eds, *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford: Hart, 2021), 211; E. Fahey, 'Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?' 8 *European*

with regard to extraterritoriality, the EU has gradually moved from being a victim to being a '(soft) perpetrator'.[38]

IV. Transnational Actors and the Extraterritorial Reach of EU Law

Data protection law has always been regarded as one of the clearest examples of the Brussels effect.[39] EU data protection law has achieved the status of the international gold standard on the basis of a particularly flexible approach to jurisdictional criteria, leading to the much-analyzed phenomenon of the 'territorial extension' of EU law.[40]

This rests on three main pillars.[41]

First, a loose interpretation of the notion of 'place of establishment' of the data processor. This was considered by Directive 95/46/EC to be the main jurisdictional basis for data processing. In the famous *Google Spain* decision,[42] the Court opted for a broad and flexible interpretation of the notion of 'establishment' (Art 4(1)(*a)* Directive 95/46/EC), which included data processing carried out by foreign operators with servers located outside of the EU,[43] but with some economic link to local branches providing auxiliar services within the internal market.

Second, the targeting of individuals or the offering of goods or services to them has been elevated by the GDPR to an autonomous jurisdictional criterium. Art 3 explicitly codifies the criterion of 'targeting' as a factor triggering the application of the Regulation 2016/679/UE, thus laying the foundations for a significant expansion of the territorial scope of the EU data protection model.[44] This criterion was justified on the basis of the (itself not uncontroversial) 'effects doctrine' of international law, according to which states can assert jurisdiction over acts committed abroad if these acts have effects in the territory of the regulating

Papers, 503 (2023).

[38] R. Bismuth, 'The European Union Experience of Extraterritoriality: When a (Willing) Victim Has Become a (Soft) Perpetrator', in A. Parrish and C. Ryngaert eds, *Research Handbook on Extraterritoriality in International Law* (Cheltenham: Edward Elgar, 2023), 118.

[39] A. Bradford, 'The Brussels Effect'107 *Northwestern University Law Review*,1 (2012).

[40] J. Scott, 'The Global Reach of EU Law', in M. Cremona and J. Scott eds, *EULaw Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford: Oxford University Press, 2019), 21.

[41] See C. Kuner, 'Data and Extraterritoriality', in A. Parrish and C. Ryngaert eds, n 38 above, 362.

[42] Case C-131/12 *Agencia Española de Protección de Datosand Costeja Gonzalez* v *Google Spain*, Judgment of 13 May 2014, available at www.eur-lex.europa.eu; see also case C-507/17 *Google* v *CNIL*, Judgment of 24 September 2019, available at www.eur-lex.europa.eu.

[43] B. Van Alsenoy and M. Koekkoek, 'Internet and Jurisdiction after *Google Spain*: the Extraterritorial Reach of the 'Right to Be Delisted' ' 5 *International Data Privacy Law*, 105 (2015); C.G. Granmar, 'Global Applicability of the GDPR in Context' 11 *International Data Privacy Law*, 225 (2021).

[44] D. Svantesson, 'The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses' 50 *Stanford Journal of International Law*, 53 (2014).

state,[45] and on the basis of the case law of the CJEU on competition law.[46] The impact of this mechanism has been significant, including in the enforcement of data subjects' rights, namely the right to be delisted.

Third, the continued application of data protection law once the data has been transferred outside of the EU. In particular, Art 25 Directive 95/46/EC allowed data transfers only if the third country ensured an 'adequate level' of data protection. The general idea behind this model is that, in line with the constitutional nature of the Directive, every individual in the EU has a right to continued protection of personal data, even when transferred to third countries.[47] Such a mechanism has been transposed into the GDPR. It formed the basis for two of the landmark rulings of the EU Court of Justice, and namely the *Schrems* 1 and 2, which struck down the agreements negotiated by the EU Commission for data transfers between the US and the EU.[48]

The EU Digital Package followed the path opened up by the data protection Regulation, not only by opting for a broad territorial scope of application, but also by extending the mechanism of continuous application of EU law even when no personal data are involved.[49]

On the first point, both Art 1(2) Digital Markets Act (DMA) (Regulation 2022/1925) and Art 2(1) Digital Services Act (DSA) (Regulation 2022/2065) enshrine the 'targeting' criterion, thus laying the foundation for the territorial extension of EU law.[50] The same is done in the Data Act (Regulation 2023/2854), in Art 1(3).[51]

[45] B. Simma and A.T. Müller, 'Exercise and Limits of Jurisdiction', in J. Crawford and M. Koskenniemi eds, *The Cambridge Companion to International Law* (Cambridge: Cambridge University Press, 2012), 134, 140.

[46] J. Scott, n 40 above,36.

[47] T. Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law* (Cham: Springer, 2023), 55.

[48] Case C-362/14 *Schrems* v *Data Protection Commissioner*, Judgment of 6 October 2015, available at www.eur-lex.europa.eu; case C-311/18 *Data Protection Commissioner* v *Facebook*, Judgment of 16 July 2020, available at www.eur-lex.europa.eu.

[49] See *amplius* F. Bignami and G. Resta, 'Extraterritoriality', in G. De Gregorio et al eds, *Oxford Handbook on Digital Constitutionalism* (Oxford: Oxford University Press, 2024) (forthcoming), available at https://tinyurl.com/5cpbsrwp (last visited 30 September 2024).

[50] Art 1(2) DMA provides: 'The Regulation shall apply to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service'. Art 2(1) DSA provides that the Regulation 'shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment'.

[51] Art 1(3) Data Act provides as follows: 'This Regulation applies to: (a) manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers; (b) users in the Union of connected products or related services as referred to in point (a); (c) data holders, irrespective of their place of establishment, that make data available to data recipients in the Union; (d) data recipients in the Union to whom data are made available; (…) (f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union; (…)'.

On the second point, both the Data Governance Act (DGA) (Regulation 2022/868) and the Data Act (on data use) extend the restrictions on the outward transfer of personal data to certain categories of non-personal data, thereby introducing a soft but effective form of data localization.[52] Interestingly, even the so-called anti-FISA clause of the GDPR (Art 48) is reproduced in Art 31 Data Governance Act and Art 32(2) Data Act.[53]

The extraterritorial reach of EU law is further reinforced by the last born of the digital regulations, and namely the AI Act. With the aim of preventing any circumvention of the prohibitions and obligations laid down by the AI regulation, and namely through re-localization strategies,[54] Art 2(1) provides for an unprecedentedly broad territorial scope of application of the Regulation.[55]

This applies not only to providers who place AI systems on the market or put them into service or to providers who place general-purpose AI models in the internal market, regardless of where they are established (lett *a)*, and to 'deployers' of AI systems who are established located in the Union (lett *b*), but also to

> 'providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system *is used* in the Union' (lett *c*).

The jurisdictional basis set out in Art 2 is so broad, in particular its lett *c,* that

[52] In particular, Art 5(9) DGA sets out a mechanism similar to the GDPR, attributing to the Commission the power to declare that a third country affords an 'essentially equivalent' protection of trade secrets and IP rights, that such protection is being effectively enforced and applied, and that effective judicial redress is available. In the absence of such declaration, data obtained for reuse cannot be transferred unless the re-user undertakes to comply with the obligations to protect IP and trade secrets, even after the data is transferred to the third country, and to accept the jurisdiction of the relevant Member State (Art 5 (10) DGA). Also, with regard to certain non-personal data declared 'highly sensitive', the Commission is empowered to adopt delegated acts supplementing the DGA by laying down special conditions applicable for transfers to third-countries; such conditions 'may include terms applicable for the transfer or technical arrangements in this regard, limitations as regards the re-use of data in third-countries or categories of persons which are entitled to transfer such data to third countries or, in exceptional cases, restrictions as regards transfers to third-countries' (Art 5 (11) DGA). Similarly, Art 32 Data Act lays down an obligation for providers of data processing services to 'Providers of data processing services shall take all adequate technical, organizational and legal measures, including contracts, in order to prevent international and third country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State'.

[53] As made clear by the Commission in the Impact Assessment Report accompanying the Data Act (European Commission, 'Impact Assessment Report accompanying the Data Act Proposal' SWD(2022) 34 final, 20-21), it is feared that foreign authorities may unlawfully access non-personal data stored in the cloud environment.

[54] See Recital 22 AI Act; A. Keane Woods, 'Digital Sovereignty + Artificial Intelligence', in A. Chander and H. Sun eds, *Data Sovereignty* n 34 above, 115.

[55] D. Bomhard and M. Merkle, 'Regulation of Artificial Intelligence: The EU Commission's Proposal of an AI Act' 10 *Journal of European Consumer and Market Law,* 257 (2021); D. Svantesson, 'The European Union Artificial Intelligence Act: Potential Implications for Australia' 47 *Alternative Law Journal*,4 (2022).

the regulation has the potential to be applied to any provider or deployer of AI systems whose outcome produces effects (by being used) in the Union. But what kind of use is required by this provision? Must the AI tool be placed in the market or deployed with the intention of being used in the Union? Or can its use in the Union be a fortuitous circumstance?

Interpreting Art 2 literally, a wide range of phenomena could fall within the scope of application of the AI Act. As Dan Svantesson points out, even a song played on the radio in Europe could raise the question of how such a song was recorded.[56] Was the voice artificially altered? Was the text or the music composed by AI? And if so, should the AI Act apply to all such activities prior to broadcasting in Europe? And, to take other examples: *i*) should an online dispute resolution system based on machine learning techniques be subject to the AI Regulation simply because one of the claimants located in Europe may be positively or negatively affected by the final decision? (*ii*)will the medical assessment of a European patient by an online screening tool made available in the US fall within the scope of Art 2?

V. Accountability of Transnational Actors and Global Power Imbalance

The long arm of European digital regulation is a paradigmatic example of the contemporary tendency to reshape the role of territory as the main criterion for justifying jurisdictional claims.[57] Territory is not abandoned altogether but increasingly reimagined so as to lose its narrow geographical boundaries.[58] As Ryngaert and Parrish put it,

> '(t)erritoriality then becomes a flexible governance technique to regulate essentially extraterritorial situations, thereby blurring the dividing line between territoriality and extraterritoriality'.[59]

However, the de-territorialization of the law does not mean that the traditional principles of sovereignty and independence of the states have been overcome. While the shift towards extraterritoriality characterizes prescriptive jurisdiction, it is much more controversial in the field of enforcement jurisdiction.[60] The experience of data protection law, and namely the difficulty of enforcing it abroad, confirms this conclusion.[61] On the other hand, extraterritoriality has always been a political

[56] ibid 8.

[57] C. Ryngaert, 'International Jurisdiction Law', in A. Parrish and C. Ryngaert eds, n 38 above, 14.

[58] M. Catanzariti, *Disconnecting Sovereignty: How Data Fragmentation Reshapes the Law* (Heidelberg: Springer, 2024); C. Ryngaert and A. Parrish, 'Introduction to the Research Handbook on Extraterritoriality in International Law', in C. Ryngaert and A. Parrish eds, n 38 above, 5.

[59] ibid

[60] C. Ryngaert, 'Extraterritorial Enforcement Jurisdiction in the Cyberspace: Normative Shifts' 24 *German Law Journal*,537 (2023).

[61] European Data Protection Board, 'Study on the Enforcement of GDPR Obligations Against

notion used to support certain normative projects,[62] and in many cases it is used as a technical tool to reinforce the paradigm of digital sovereignty.

As a result of this evolution, transnational actors are increasingly caught up in a dense – and often contradictory – web of local, regional, and supranational regulations. This circumstance, together with the reputational and market pressure mentioned above, may contribute to subjecting to subjecting the new technocratic powers to at least limited forms of legal control. From this perspective, such a development may be seen as desirable, and indeed extraterritoriality has often been defended as a tool to achieve global justice projects.[63] However, one should not underestimate the downsides of the contemporary fascination with extraterritoriality.

First, there may be serious jurisdictional conflicts. Compare, for example, the US Cloud Act – which allows US authorities to obtain data stored by providers under US jurisdiction, regardless of whether the servers are located in the US or abroad – with Art 48 GDPR (and Art 32(2) Data Act) – which prevents providers from transferring personal data to authorities in third-countries even if such transfers are authorized or ordered by a decision of a foreign court, tribunal, or administrative authority.[64]

Second, it may increase the accountability of powers in one geopolitical scenario, but it may also exacerbate the already strong asymmetries in North/South relationships. It cannot be overlooked that by extending the geographical scope of domestic law, any legislation ends up significantly increasing the compliance burden for any actor within the reach of the relevant regulation, regardless of their location. Consider, for example, the obligation to appoint a representative in the EU, under Art 27 GDPR and Art 22 AI Act. This is a formality for multinational platforms but becomes a huge cost when applied to a smaller company from a developing country. From this perspective, regulation risks amplifying the already strong technological imbalance between North (or North-East) and South, by introducing digital trade barriers for developing countries.[65]

This is the criticism that is often made in terms of 'data (or digital) colonialism',[66]

Entities Established Outside the EEA but Falling under Article 3(2) GDPR', Brussels, 2021.

[62] C. Ryngaert and A. Parrish, 'Introduction' n 58 above, 6.

[63] See for instance E. Benvenisti and G. Nolte eds, *Community Interests Across International Law* (Oxford: Oxford University Press, 2018); M. Langford et al eds, *Global Justice, State Duties: The Extraterritorial Scope of Economic, Social, and Cultural Rights in International Law* (Cambridge: Cambridge University Press, 2012).

[64] See J. Daskal, 'The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU-US Discussions Regarding Law Enforcement Access to Data Across Borders', in F. Bignami ed, *EU Law in Populist Times: Crises and Prospects* (Cambridge: Cambridge University Press, 2020), 319.

[65] A. Renda, 'Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy' 14, available at https://tinyurl.com/3yvh73e9 (last visited 30 September 2024).

[66] C. Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets' 53 *Vanderbilt Journal of Transnational Law*, 685 (2020); S. Calzati, "Data Sovereignty' or 'Data Colonialism'? Exploring the Chinese involvement in Africa's ICTs: A Document Review on Kenya' 40 *Journal of Contemporary African Studies*, 270 (2022); D. Coleman, 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the

and which is echoed in some chapters of the book.[67]

Such a critique should be seriously considered and should not obscured by the rhetoric that surrounds much of the EU's recent digital regulation, which oscillates between an emotional call for a human-centred regulation[68] and a pragmatic claim to strategic independence.[69] As Dan Svantesson convincingly argues,

> 'if we want a more level playing field between the developed and the developing countries, scalability must be a consideration when the powerful and most influential countries and regions implement new legal approaches'.[70]

Limitations of Data Protection Laws'24 *Michigan Journal of Race & Law*, 417 (2019); U. Sahbaz, 'Artificial Intelligence and the Risk of New Colonialism' (14) *Horizons: Journal of International Relations and Sustainable Development*, 58 (2019); J. Muldoon and B.A. Wu, 'Artificial Intelligence in the Colonial Matrix of Power' 36 *Philosophy and Technology*, 80 (2023).

[67] R. Gottardo, n 17 above, 174; S. Mancuso and L. Corselli, 'Profiling in Algorithm-Based Decisions: An African Perspective', in M. Bussani et al eds, *Comparative Legal Metrics* n 1 above, 249-264.

[68] See L. Floridi, 'The European Legislation on AI: A Brief Analysis of its Philosophical Approach' 34 *Philosophy and Technology*, 215, 216-217 (2021).

[69] European Commission Communication of 19 February 2020on a European Strategy for Data COM(2020) 66 final.

[70] D. Svantesson, 'The European Union Artificial Intelligence Act' n 55 above, 8.