Giovanni Maria Riccio[*]

Brussels Effect, Data Protection and AI Act

This article explores the role of comparative law in understanding and addressing the legal challenges posed by emerging technologies. It addresses the following issues: the reasons why the European Union sets global regulatory standards, illustrated by the example of the GDPR; the factors behind the United States' capacity for innovation; and the potential future circulation of the EU legal model.

Keywords: *Data Protection, European Union, GDPR, regulatory law, private law, AI Act, Brussels Effect, legal fragmentation, neoliberalism, digital markets, Chinese tech companies, compliance challenges.*

1. The Usefulness of Comparative Law in the Study of Emerging Technologies

Addressing the topic of artificial intelligence from a comparative legal perspective is no easy task. It requires, as a preliminary step and in order not to create unrealistic expectations for readers, a clarification of the analytical scope. Those seeking detailed information on the specific regulations of various legal systems should be advised to stop reading and turn to more profitable activities.

Indeed, it should be common knowledge—though it bears repeating—that comparative law is essentially a method, even if the scholarly debate on the methods and functions of comparative legal studies appears to be losing momentum[1]. However, we can certainly say what comparative law is *not*: it is *not* the study of foreign legal systems per se, nor is it merely a compilation of legal information—it is, above all, comparison[2].

---

[*]Founder and Senior Partner at e-Lex Law Firm (Rome); Full Professor of Comparative Law; Current courses: Copyright Law, Cultural Heritage Law, Art Law - Università di Salerno/DPO.

[1] For an introduction to this aspect, see *Stanzione P.*, Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974, XXIII, also in French on in Rev. *int. droit comparé*, 1973, 885; L.-J. Costantinesco, Il metodo comparativo, ed. it., Torino, 2000.

[2] According to *Sacco R.*, Circolazione e mutazione dei modelli giuridici, in Dig disc. priv., sez. civ., II, Torino, 1988, 365, If comparative law were merely the analysis of foreign legal systems, its function would be limited to a descriptive exercise, lacking any real impact on the understanding and development of domestic law. Instead, comparative law offers a method for critically examining one's own legal system, revealing not only its distinctive

Comparative law does, of course, serve to explore alternative solutions, but it is also a valuable tool for deepening our understanding of domestic law. It does not confine itself to the analysis of legislative texts but aspires to move beyond legal formalism. It begins with the study recent decades, even identifying these formants—or rather, outlining their boundaries—has become increasingly complex. Consider, for example, the legislative formant national law, supranational law, and the decisions and measures issued by independent administrative authorities all now coexist and interact.

For decades now, we have been witnessing the rise of polycentric law, resulting from the erosion of the state's monopoly over the production of legal norms[3]. This is a product of economic globalization, where national legislative sovereignty must now coexist with new centers of legal norm production, including international economic and professional communities[4]. Sometimes this law is not imposed from above but emerges spontaneously from international commercial practices; other times, it is state law enriched with prescriptive content from private rules—as is the case with references to harmonized standards in the AI Act[5].

It is enough to observe that most legal norms governing innovation today originate from the European Union, including those related to artificial intelligence. At the Union level, there has been a marked shift away from directives in favor of regulations, signaling a transition from legal harmonization to uniformization. This choice reflects, among other factors, the desire of some national legal systems to preserve their own legislative sovereignty—often in response to political or lobbying pressures—which, however, risks undermining the EU's stated objective in this field: the creation of a barrier-free internal market that realizes the core aims of the Treaties.

features but also its potential shortcomings or inefficiencies in comparison with alternative legal models. (Still *Sacco R.*, Introduzione al diritto comparato, in Tratt. dir. comp. dir., da R. Sacco, 5ª ed., Torino, 1992).

[3] Cf. *Ferrajoli L.*, Crisi del diritto e dei diritti nell'età della globalizzazione, in Questione Giustizia, 2023, <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>.

[4] Here too, the bibliography could be vast; however, for a methodological analysis as well, reference is made to *Grossi P.*, Aspetti giuridici della globalizzazione economica, in I Georgofili. Atti della Accademia dei Georgofili» 2013.

[5] The harmonized standard, according to Regulation (EU) No 1025/2012, is a technical specification adopted by a European standardization body (for example, CEN – the European Committee for Standardization; CENELEC – the European Committee for Electrotechnical Standardization; ETSI – the European Telecommunications Standards Institute) based on a request made by the European Commission. These standards are developed to facilitate the implementation of European Union legislation and to ensure a more efficient single market. The process of creating a harmonized standard involves several steps. First, the European Commission issues a mandate identifying a regulatory need and entrusts one of the European standardization bodies (CEN, CENELEC, or ETSI) with the task of drafting a specific standard. These bodies then develop the standard, involving technical experts and stakeholders in the drafting process to ensure the standard meets market needs and complies with EU legislation. Finally, the standard is adopted and published in the Official Journal of the European Union. However, Recital 117 introduces an additional requirement, stating that the harmonized standard must be "considered suitable for governing the relevant obligations by the AI Office." Therefore, it must be understood that, in addition to the Commission's mandate, a subsequent "endorsement" by the AI Office is required in order for the harmonized standard to benefit from the presumption of conformity.

Moreover—and again this is common knowledge among comparatists—the analysis of legal formants must necessarily be coupled with that of crypotypes[6]: the constellation of elements—linked to a people's legal tradition, modes of knowledge transmission, social and cultural context, and economic environment—that shape the training and worldview of legal professionals. This becomes particularly important when moving beyond the Western Legal Tradition. As the legal regulation of AI technologies inevitably requires, we often encounter non-Western legal systems whose lawyers and policymakers are shaped by a distinct hierarchy of values—one that may differ significantly from that of their Western counterparts.

Nor can we overlook, especially in the context of regulating AI systems, the increasingly central role played by ethics, which ought to guide the design of such systems in order to avoid discriminatory biases or exploitations contrary to the shared values of the international community. On this point, it is important to note that the semantic scope of the term "etica" (ethics) in romance languages does not entirely overlap with the broader Anglo-American concept of "ethics": in the former, ethics has primarily a subjective connotation, separate from legal norms, which follow formal criteria for their selection; in the latter, ethics is more expansive, often embedded in forms of soft law, such as codes of ethics or conduct.

To define comparative law as a method is to recognize that it goes beyond mere data collection on foreign legal systems[7]. This legal field does not simply involve listing and analyzing rules from different countries, but rather focuses on identifying the structures, principles, and solutions adopted within various legal contexts. In this paper, we aim to outline some of the main features that characterize the European and U.S. systems. For reasons of brevity, we will deliberately set aside the insights that might emerge from an analysis of Asian legal systems. We will not focus on individual legal institutions but instead seek to identify prevailing elements that underlie legal policy choices.

This approach stems from an awareness of the profound transformation of legal systems over the last thirty years. In an era of growing interconnection among states, comparative law plays an increasingly crucial role, as legal systems no longer exist in isolation but continuously interact through international treaties, supranational institutions, and processes of legal reception and harmonization[8].

[6] Cryptotypes, in comparative law, are those implicit elements of a legal system that do not find direct expression in the formal sources of law (legislation, case law, and doctrine) but deeply influence the functioning and application of norms. They include cultural values, established practices, legal mindsets, and unwritten principles that determine how law is interpreted and applied in a given society. The concept of cryptotypes was developed by Rodolfo Sacco, who highlighted how, alongside explicit formants, there exist these latent elements that shape the law of a legal order. They are particularly relevant when analyzing legal systems belonging to different traditions, as they allow for an understanding of the real legal dynamics beyond the normative data.

[7] *Gorla G.*, Diritto comparato, in Enc. dir., XII, Milano, 1964, 930; *Ascarelli T.*, Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952, 6 ss.

[8] *Mattei U.*, Comparative Law and Economics, Univ. of Michigan Press, 1997; *Hoecke Van M.*, Epistemology and Methodology of Comparative Law, Hart Publishing, 2004; *Zeno-Zencovich V.,* Comparison Involves Pluralism*:* A Rejected View-Point, in Comparative Law Rev., 2025, 6.

Finally, the comparative approach requires a rejection of formalism and a move beyond the mere analysis of legislation. It calls for consideration of the many factors influencing the creation and application of law, including extra-legal reasons, the interplay among different legal formants, and their mutual influence. For this reason, as anticipated, we will focus on comparing the political (and thus legal) rationales behind the different regulatory approaches adopted in the field of artificial intelligence.

2. Why the European Union Makes the Rules: The Example of the GDPR

A pervasive narrative has taken hold in mass media rhetoric—one that is highly reductive and lacks empirical support—claiming that the United States innovates, China copies, and the European Union regulates. Beyond the oversimplification, this assertion deserves closer examination to understand the reasoning behind such a classification.

Let us begin at the end—that is, with the idea that Europe invests little in innovation but excels in producing legal norms.

This assumption is misleading when viewed in percentage terms, but unfortunately realistic in absolute terms. A recent edition of the EU Industrial R&D Investment Scoreboard, published in December 2024, reported that in 2023, European industry outpaced the growth of U.S. (+5.9%) and Chinese (+9.6%) companies for the first time, with a growth rate of 9.8%.

While encouraging, this figure does not account for three important factors.

First, the wide disparities among EU Member States, with higher peaks in more advanced countries like France and Germany, while others—including Italy—lag behind; second, that these percentages refer to vastly different absolute values; and third, that European investments are often spread across many small-scale projects rather than concentrated in a few strategic initiatives. The Horizon 2020 programme is a case in point: it funded numerous small entrepreneurial ventures, not all of which yielded industrial outcomes.

Then there is the matter of regulation, grounded in the concept—now widely known and perhaps declining—of the so-called Brussels Effect. This refers to the EU's ability to project its regulatory influence beyond its geographic and jurisdictional borders, shaping business practices, national legal frameworks, and even international agreements.

A central pillar of the Brussels Effect[9] is the extraterritorial application of EU law: regulations apply not only to entities based within the Union, but also to those outside

[9] The term is due to *Bradford A.*, The Brussels Effect: How the European Union Rules the World, Oxford Univ. Press, 2020. The author identifies the key to this regulatory influence in the size of the European internal market, combined with strong regulatory capacity: to access the EU market, global companies comply with European standards, ultimately applying them also in other markets, producing a de facto harmonization effect. The book

it that offer goods or services within the EU market or process data of EU citizens. The most paradigmatic example is the General Data Protection Regulation (GDPR), which applies to data controllers outside the EU whenever they process personal data of individuals located within the Union (Art. 3 GDPR). This creates a need for many non-EU companies to adapt their data practices to EU standards. This normative reach is justified both by the effects doctrine under international law and by the EU's market power, whereby access to the internal market requires compliance with its rules[10].

Beyond formal extraterritoriality, global companies frequently adopt EU standards voluntarily—or more precisely, *de facto*—for reasons of regulatory consistency and economic efficiency. It is often simpler to adhere to a single, stringent standard—typically the EU one—rather than customize compliance for each market. This is especially true in areas like environmental protection, food safety, privacy, and competition law.

Once again, the GDPR provides a clear example: tech giants like Google, Apple, and Microsoft have adopted GDPR-inspired data protection policies globally, even in contexts where they are not formally required to do so. Similarly, in the environmental field, Japanese and U.S. automakers have aligned their emission standards with EU requirements to maintain market access, often extending those standards globally[11].

Another vector of the Brussels Effect is regulatory imitation by third countries that lack the economic clout of the United States. The technical quality, internal coherence, and market-driving effect of EU rules have made them a model for many national legislations. Imitation may stem from pragmatic goals (e.g. facilitating EU market access) but also from legal prestige and a desire for normative convergence.

---

shows how this occurs in strategic sectors such as personal data protection (GDPR), food safety, competition, environmental sustainability, and finance, building a narrative according to which the Union acts as a "regulatory superpower," capable of setting the global rules of the game despite lacking an explicit imperial or coercive strategy. The analysis is distinguished by its legal-economic approach, but also by a political reading that recognizes European regulatory power as a form of institutional soft power, founded on technocracy, procedural transparency, and the attractiveness of the European regulatory model. The Brussels Effect thus emerges as a predominantly unilateral process, not the result of multilateral negotiations, but rather of the EU's structural power and the economic rationality of global companies.

[10] *Bradford A., note* 9, 5: "the EU can unilaterally externalize its laws outside its borders through market mechanisms".

[11] The Brussels Effect also extends to the international level, both through the spread of European standards in multilateral trade agreements and through their adoption in technical standards by supranational organizations such as ISO (International Organization for Standardization), the Codex Alimentarius Commission, or ICAO (International Civil Aviation Organization). In the context of trade agreements, the EU has often included regulatory clauses that require the adoption of European standards or equivalent ones. This is the case with Association Agreements or free trade agreements (e.g., CETA with Canada, EPA with Japan), which include provisions on environmental sustainability, data protection, and product safety. In such agreements, the EU imposes minimum requirements, helping to extend its standards to third countries. Beyond the legal framework, it is important to highlight how the Brussels Effect also manifests informally and technically through the definition of harmonized rules and industrial norms. Many European technical standards become global practice due to their rigor and practical usefulness. Multinational companies adopt them to avoid the risk of having to design differentiated products for different markets. The spread of technical standards can be further facilitated by soft law—that is, non-binding instruments (guidelines, recommendations, codes of conduct) produced by European agencies or standardization bodies. The example of the codes of conduct provided for by the GDPR (Articles 40–41), although not mandatory, shows how these tools can act as catalysts for regulatory convergence, especially in technological or digital sectors.

The most fertile ground for this effect has been data protection law. But in environmental law too, the EU's regulation of chemicals (REACH) has served as a model for countries like China and Turkey, fueling a phenomenon of unilateral regulatory globalization—not through imposition, but through voluntary alignment with EU standards, for reasons of compatibility and strategic advantage[12].

In the case of the GDPR, imitation has ranged from literal replication to selective adoption—most notably of the accountability principle under Art. 5(2), which requires the controller (the entity determining the purposes and means of processing) to ensure that fundamental data protection principles—lawfulness, fairness, transparency, data minimization, integrity, etc.—are upheld not through a fixed list of obligations, but by demonstrating that processing ensures adequate protection of data subjects' rights and freedoms.

For example, Brazil's Lei Geral de Proteção de Dados (LGPD)—Law No. 13.709 of 2018—bears strong resemblance to the GDPR[13]: it applies to all entities (public or private, natural or legal) that process personal data of individuals located in Brazil, regardless of the data controller's location; it requires clear and comprehensive disclosure to data subjects; mandates impact assessments for high-risk processing; and obliges maintenance of a processing activity register[14].

Article 50 of the LGPD allows controllers and processors—individually or via associations—to develop codes of good practice and governance, internal oversight mechanisms, risk mitigation strategies, and especially technical and security standards. On this point, the LGPD and GDPR diverge: while the latter allows for the drafting of codes of conduct, it does not clearly regulate the definition of common technical and security standards, leaving operators with some uncertainty regarding best practices.

Brazilian law further provides that data governance policies should be based on a systematic risk-impact assessment, proportionate to the organization's size, scope of activities, and data sensitivity. Like the GDPR, Article 50 of the LGPD requires controllers to demonstrate the adequacy of adopted measures; however, the inclusion of a minimum baseline of mandatory safeguards arguably makes compliance easier—at least procedurally—for Brazilian companies and administrations.

A similar comparative analysis applies to Switzerland's revised data protection law, which came into force in 2020 after a legislative process that began in 2017. Among other elements, legal persons are no longer included in the definition of "personal data"; as in Brazil, controllers must keep a processing register; impact

[12] See *Almada M., Petit N.,* The EU AI Act: A Medley of Product Safety and Fundamental Rights, EUI, RSC, Working Paper, 2023/59.

[13] *Liz dos Santos A.L.*, Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais", Revista dos Tribunais, (2020), 105.

[14] For further details, see *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in *Souza C.A., Magrani E., Silva P., (eds.),* Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.

assessments are required for high-risk processing; and personal data breaches must be reported to the supervisory authority (the Federal Data Protection and Information Commissioner)[15].

Swiss law also mandates the appointment of a local representative for controllers based abroad. Regarding data subject rights, the new law introduces, in line with the GDPR, the right to data portability and the right not to be subject to solely automated decisions. It also incorporates privacy by design and by default, as well as data minimization principles. The supervisory authority's powers have been expanded to include inspections and binding decisions.

Many other countries have adopted GDPR-inspired regulations, including Nigeria's Data Protection Regulation (NDPR), issued in January 2019, and Egypt's Law No. 151 of 2020. For smaller nations, this reflects a clear desire to facilitate trade with the EU, beyond the legal prestige the GDPR has clearly achieved. Switzerland's alignment seems almost inevitable, given its geographic location, though it remains outside the EU. What is more surprising is that a global economic power like Brazil has adopted such similar standards.

A separate—albeit brief—treatment is warranted for China's data protection reform. The Personal Information Protection Law (PIPL) came into force on November 1, 2021, after a lengthy legislative debate. It likely represents a major shift in the global legal landscape, as China has adopted several EU-inspired regulatory elements, replicating many GDPR provisions[16].

The law's scope covers three primary scenarios:

a) Processing activities carried out within China;
b) Provision of goods or services to Chinese citizens, or analysis of their behavior;
c) Other cases specified in national laws.

When a foreign entity processes personal data under PIPL's jurisdiction, Article 53 requires it to establish a presence in China or appoint a representative, whose details must be submitted to the authorities. Article 72 echoes the GDPR by exempting personal or domestic data processing from PIPL's scope.

The PIPL mirrors the GDPR in distinguishing between data controllers and processors, assigning them similar roles: controllers determine the purposes and means of processing; processors act under their direction. Strong parallels also emerge regarding the required information at the point of data collection, closely resembling Article 13 of the GDPR[17].

Sensitive data under PIPL includes religious beliefs and health data (as in the GDPR), but also financial information and personal assets—categories not classified as sensitive under EU law. Biometric data, information about minors under 14, and

[15] Cf. *Meier P., Métille S.,* Loi fédérale sur la protection des données, Helbing Lichtenhahn Verlag, 2023.

[16] *Moriconi C.*, Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China, 9 Nordic Journal of Law and Social Research, (2019) 248; *Santoni G.*, Personal data as a market commodity: legal irritants from China "experience", 1 European Journal of Privacy Law and Technology, (2023), 1.

[17] *Creemers R.*, China's Emerging Data Protection Framework, (November 16, 2021), SSRN: https://ssrn.com/abstract=3964684.

geolocation data are all expressly included among sensitive categories—highlighting heightened global concern.

The legal bases for data processing under PIPL strongly resemble those in the GDPR. Consent must be freely given, specific, and revocable (Article 14). Like the GDPR, consent is not required if data processing is necessary for contractual obligations or legal compliance. Public health emergencies and life-or-death scenarios are also recognized as valid legal bases[18].

PIPL places significant emphasis on data transfers, requiring prior assessment procedures akin to the GDPR's DPIA—but with stricter conditions[19]. These assessments must evaluate the validity, necessity, and proportionality of the transfer; data categories and sensitivity; and the recipient's technical and organizational safeguards[20].

Article 40 requires these assessments to be carried out by the State Department for Cyberspace Administration and based primarily on security criteria. The obligation applies to critical infrastructure operators and controllers processing personal data above thresholds set by the same Department.

The major difference between the EU and Chinese models lies in the authority responsible for evaluation. In China, self-assessment is not permitted: public authorities must validate all measures, following uniform standards. In contrast, the GDPR gives controllers the freedom to adopt what they deem appropriate safeguards. In this sense, China's model appears more predictable—*formally*—but it also entails constant state surveillance of information flows.

The GDPR-PIPL parallel breaks down when shifting from private to public law, particularly in the relationship between state and citizens. The PIPL seems to move along two tracks: on the one hand, aligning with EU rules to facilitate commercial exchanges; on the other, preserving a clear distance in terms of public law approach[21].

[18] *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL), 5 Smart Cities, (2022) 1140.

[19] Article 38 of the PIPL (Personal Information Protection Law) provides four distinct and alternative criteria for the transfer of personal data abroad: a) Passing a security assessment organized by the national Cyberspace Administration of China, in accordance with Article 40 of this law; b) Obtaining a personal information protection certification issued by a specialized body according to the provisions of the national Cyberspace Administration of China; c) Entering into a contract with the foreign recipient based on a standard contract formulated by the same Administration, which establishes the rights and obligations of both parties; d) Other conditions stipulated by laws or administrative regulations, or by the national Cyberspace Administration of China. The translation of the PIPL was made by Rogier Creemers and Graham Webster, based on the preliminary English version of the second draft revision of the law developed by DigiChina, and is available at the following link: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ For further discussion on the assessment to be conducted, see also *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.

[20] *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.

[21] Cfr. *Pernot-Leplay E.,* China's Approach on Data Privacy fLaw: A Third Way between the US and the EU? 49 Penn State Journal of Law & International Affairs, (2020) 49, secondo cui la Cina rappresenterebbe un modello terzo rispetto a Stati Uniti ed Europa.

For instance, the definition of "sensitive data" includes any information whose unlawful disclosure might harm dignity, national security, or personal property—reflecting a stark imbalance between individuals and state authority. A special category—absent from EU law—covers data processing for journalistic, political, or public interest purposes.

Lastly, it is worth noting that PIPL does not hold a central position in China's digital regulatory framework as GDPR does in the EU. Rather, it is embedded within a broader legal architecture dominated by cybersecurity law. In a system where fundamental rights are subordinate to other state priorities, personal data protection remains a secondary concern.

3. Why the United States Innovates (or Would Innovate)

Let us now return to the initial assumption that the United States plays the role of the "great innovator" by analyzing the legislative approach that has supported technological development. While it is undeniable that the level of technological advancement among U.S. companies is unmatched by other countries, it is equally clear that political and legislative choices have significantly influenced this development.

The neoliberal rhetoric underpinning these choices has always relied on a core assumption: "technology changes exponentially, but social, economic, and legal systems change incrementally."[22] This introduces a problem of "pace," meaning that law evolves more slowly than technological progress, and thus institutions should refrain from imposing constraints on digital innovation until technologies have fully matured. However, this simplification deserves scrutiny. While it is true that technology moves faster than legislative processes, it is also true that the function of the law should be not only to drive technology forward but also to impose limits when technological developments endanger recognized and codified values.

The most insightful scholarship has referred to a "twentieth-century synthesis"—a neoliberal paradigm based on three key pillars: market efficiency as the supreme criterion, which overlooks issues of power and inequality; formal neutrality of legal

[22] These are the words of *Downes L.,* The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009. The book analyzes the impact of digital technologies on law and society, starting from the thesis that law and regulatory institutions evolve at a linear pace, while technology advances exponentially. This imbalance generates a regulatory disruption, where traditional legal rules struggle to adapt to new digital scenarios, giving rise to the nine "laws of disruption." These laws highlight how technology upends established sectors, rendering obsolete legal norms that were created in pre-digital eras. Issues such as privacy, intellectual property, platform liability, and data governance are addressed proactively, with a call to develop a more flexible, principle-based regulation capable of evolving alongside innovation. It is worth noting that, beyond influencing U.S. regulatory solutions, the book has had a significant impact on academic and policy debates concerning the need for agile and adaptive regulation. In fact, although not directly cited in legislative texts, this theory has contributed to shaping the European Union's legislative choices toward risk-based and technologically neutral approaches, as reflected in the GDPR, the Digital Markets Act, and the AI Act.

rules, which conceals underlying power dynamics; and an "anti-political" approach that reduces the role of democratic politics in favor of technical decision-making[23].

Furthermore, the adoption of law & economics paradigms and their doctrines—which dominated North American debates for decades—has shaped the very pillars of neoliberalism. Neoliberalism should not be seen as a natural outcome of market logic, as is often claimed or assumed, but rather as an institutional force shaped by law. Here, legislative and judicial components do not play a neutral role; they actively contribute to structuring markets, strengthening private powers, and influencing democratic capacity[24].

It is no coincidence that, in the United States—where no federal data protection regulation exists—legal scholarship still tends to define privacy as the "right to be let alone," rather than as control over the circulation and use of personal data. In other words, the U.S. remains far removed from the European paradigm of data protection as a fundamental right, and still clings to a proprietary notion of privacy—as a right to exclude others from one's private affairs or a proprietary control over one's own data. This approach fails to consider that the use of data, while aimed at protecting the individual, must give way to the collective interest when super-individual concerns arise[25].

In the field of artificial intelligence, a confused debate is currently underway between those advocating for a complete moratorium on any new regulation (even suggesting that existing laws be suspended for the next decade), and others—more cautiously—insisting on the need to establish safeguards and protections for citizens in the face of emerging technologies. The risk is a new phase of laissez-faire, allowing American companies to consolidate (or rather, strengthen) their oligopolistic positions in the market, unburdened by transaction costs or regulatory hurdles. This scenario recalls the late 1990s and early 2000s—the first "season" of the internet.

Analyzing the U.S. legal model is complicated by its federal nature and the resulting constellation of often-inconsistent state-level laws regulating technological innovation.

---

[23] See *Purdy J.S., Grewal D.S., Kapczynski A., Rahman S. K.*, Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis, 129 Yale L.J. 1784, 2020. This is, in our opinion, a seminal study, as it theorizes the so-called Law and Political Economy (LPE) approach. It challenges the dominant view that law should merely ensure neutral market conditions while allowing economic actors to operate freely without structural interference from the state—a view that proves inadequate for understanding contemporary dynamics of inequality, economic power, and democratic crisis. The authors argue that law is never neutral; rather, it plays a constitutive role in organizing the economy and distributing resources and power. The article calls for a rethinking of legal institutions as tools for social transformation, promoting economic justice, inclusion, and substantive democracy. It has significantly influenced academic debate, particularly in areas such as digital regulation, labor, environmental law, and racial equity.

[24] Cf. *Kennedy D.*, Law-and-Economics from the Perspective of Critical Legal Studies, in P. Newman (ed.), The New Palgrave Dictionary of Economics and the Law, London, 2002, <duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>.

[25] A paradigmatic example is the undoubtedly valuable and scientifically rigorous work by *Richards N.,* Why Privacy Matters, Oxford University Press, 2021.

However, two examples are paradigmatic.

In 1996, the *Communications Decency Act* (CDA) was enacted under the Clinton administration as a response to the growing issue of child pornography online[26]. Senator Exon, the Act's main proponent, intended to curb the proliferation of online pornography and, in particular, to restrict minors' access to such content[27]. The potential threat posed by the internet—as a sort of red-light district—prompted the creation of this Act, which was heavily criticized by scholars as a liberticidal measure against internet development (and ultimately challenged before the Supreme Court in *Reno v. ACLU*)[28].

One key provision was the *Good Samaritan Clause*—§ 230(c)(2)(A)—which granted immunity to internet service providers (ISPs) acting in good faith to restrict access to material deemed obscene, offensive, or otherwise harmful, even in the absence of specific constitutional protections. Over time, this clause not only influenced defamation law but also became a legal shield for ISPs to avoid removing user-posted content.

[26] Following the adoption of the Act under consideration, part of the legal scholarship proposed an alternative solution for the regulation of online pornography assigning websites a second-level domain (e.g., .sex or .osc) capable of indicating, *prima facie*, the obscene nature of the content. See *Major A. M., Internet Red Light District:* A Domain Name Proposal for Regulatory Zoning of Obscene Content, in *Marshall J.* Computer & Info. 21, 1997.

[27] "The information superhighway should not become a red-light district. This legislation will keep that from happening and extend the standards of decency, which have protected telephone users to new telecommunications devices. Once passed, our children and families will be better protected from those who would electronically cruise the digital world to engage children in inappropriate communications and introductions. The Decency Act will also clearly protect citizens from electronic stalking and protect the sanctuary of the home from uninvited indecencies", 141 Cong. Rec. S1953. See also "The fundamental purpose of the Communications Decency Act is to provide much needed protection for children," 141 Cong. Rec. S8088. The legislative proposal was inspired by a study by M.R. Imm, Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories, 83 Georgetown L.J. 1849 (1985), which claimed that 83.5% of content distributed online was pornographic in nature. The study, however, raised significant concerns among both U.S. legal scholars and system operators. For a summary of the criticisms, see *Cannon R*., The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 Fed. Comm. L.J. 52 (1996). On the subject of obscenity, the leading precedents include Miller v. California, 413 U.S. 15 (1973), which established the standards for evaluating obscenity (the so-called obscenity test), and Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973), which recognized the State's interest in regulating the commercial distribution of obscene and pornographic materials, as well as public performances of such nature. At the legislative level, obscenity is governed by Chapter 71 of Title 18 of the United States Code, while § 223 of Title 47 addresses "Obscene or Harassing Telephone Calls." It is worth recalling that obscenity is one of the rare forms of speech not protected by the First Amendment. Naturally, the possession and distribution of child pornography are also prohibited; see 18 U.S.C. § 2251; Osborne v. Ohio, 495 U.S. 103 (1990). Finally, in 1998, the Protection of Children from Sexual Predators Act was enacted to combat online child exploitation.

[28] 521 U.S. 844 (1997). The Supreme Court struck down only §§ 223 (a) and (d) of the law, which prohibited "the knowing transmission of obscene or indecent messages to any recipient under 18 years of age" and "the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age." It should also be noted that in 2001, the Children's Internet Protection Act and the Neighborhood Internet Protection Act came into force. These laws require library operators to install filtering software on their computers that provide internet access to users, in order to block the display of pornographic material.

In retrospect, § 230—despite its excesses—enabled the expansion of services offered by the then-new internet players, who benefited from a kind of immunity by not being required to remove third-party content.

A second significant example is the *Digital Millennium Copyright Act* (DMCA) of 1998, which introduced provisions to protect ISPs from copyright infringement claims, affirming the principle of technological neutrality—later mirrored in the EU E-Commerce Directive (2000/31/EC)[29].

The DMCA rules—subsequently adopted in the EU—exempted ISPs from liability for illegal content uploaded by users, provided such content was promptly removed following a valid takedown notice. These guarantees indisputably contributed to the rise of platforms like YouTube, Facebook, and other digital intermediaries by allowing them to host vast quantities of user-generated content without prior control—thereby laying the foundation for the global dominance of U.S. Big Tech in the digital economy.

Today, regarding AI regulation, U.S. companies once again hold a dominant position in the market, and policy is responding accordingly, with a push toward *non-regulation* rather than mere *deregulation*. A recent example is the attempt to introduce a ten-year moratorium on any state or local AI regulation, with the explicit goal of avoiding constraints on AI development and giving the industry a free hand to compete globally—particularly against China, a favorite target of Trump-era policies. This ban was included in the *Big Beautiful Bill* (H.R.1), a tax and infrastructure reconciliation bill, with strong backing from major tech firms who argued that a uniform federal framework would be more efficient than a fragmented patchwork of state laws[30].

This moratorium—applying to AI systems, algorithmic models, or automated decision-making tools—was meant not only to block new laws but also to nullify existing ones, effectively transferring all regulatory power to Congress. According to its proponents, this would reduce legal fragmentation among single states.

However, the proposal was overwhelmingly rejected by the Senate with a bipartisan 99-to-1 vote. It must be noted, though, that this outcome was less about a principled rejection of AI deregulation and more about a Republican inclination to

[29] See *Verbiest T., Spindler G., Riccio G.M.,* Study on the Liability of Internet Intermediaries, European Commission, DG Internal Market, 22007, SSRN: <https://ssrn.com/abstract=2575069 or http://dx.doi.org/10.2139/ssrn.2575069>, 2002, and more recently *Geiger C., Frosio G., Izyumenko E.,* The Oxford Handbook of Online Intermediary Liability, Oxford University Press, 2020.

[30] In particular, see the statements made by Sam Altman and reported by Tech Policy Press, *Transcript*: Sam Altman Testifies at US Senate Hearing on AI Competitiveness, https://www.techpolicy.press/transcript-sam-altman-testifies-at-us-senate-hearing-on-ai-competitiveness/. Specifically, the entrepreneur rejected proposals requiring developers to obtain government approval before releasing AI systems, calling them "disastrous" for the sector. He nonetheless emphasized that the establishment of standards by NIST (National Institute of Standards and Technology) could be useful, provided it does not slow down progress. Moreover, while acknowledging the United States' technological edge over China, he argued that this lead is difficult to assess from a forward-looking perspective. To reinforce this point, he concluded that the future of AI must be grounded in "democratic values such as transparency and freedom," setting itself apart from authoritarian models.

preserve the autonomy of individual states. In other words, the rejection reflected concerns over the federal-state relationship and administrative discretion, rather than an effort to prevent unregulated AI development.

Still, while this case does not demonstrate a clear stance on AI policy, it shows that the winds in U.S. regulation may be shifting.

As recently observed, the Biden administration's strategy unfolded in two phases[31]. The first, more programmatic phase included the publication of the *Blueprint for an AI Bill of Rights* in 2022—a non-binding document outlining core principles for responsible AI use: protection from surveillance, algorithmic transparency, non-discrimination, and accountability. The second, more operational phase came with *Executive Order 14110* of October 30, 2023[32], which imposed binding obligations on developers of advanced AI models, particularly dual-use systems, adopting a holistic approach that integrates national security, civil rights protection, and innovation promotion.

While this Executive Order did not create direct federal legislation, it outlined a detailed set of obligations, guidelines, and directives for federal agencies, aiming to balance technological innovation with national security and civil liberties. Several of its core principles aligned with those of the European *Artificial Intelligence Act*. For instance, the order mandated transparency obligations for companies developing high-impact foundation models—particularly those exceeding certain thresholds of computational capacity or trained on large datasets of non-public information. These thresholds were defined by the Department of Commerce, via the National Institute of Standards and Technology (NIST), in collaboration with other technical and security agencies.

Further parallels include obligations around transparency and combating deepfakes, involving experimentation with watermarking and content traceability technologies, the development of technical standards for identifying AI-generated content, and the creation of provenance protocols to strengthen public trust in digital information.

However, with Trump's return to the presidency in January 2025, there was a substantial shift in regulatory direction. This began with *Executive Order 14179*, which fully revoked Biden's order and directed federal agencies to review and eliminate regulations deemed to hinder AI development. Trump's approach, clearly grounded in deregulatory principles, seeks to reassert U.S. technological leadership by eliminating constraints perceived as ideological or anti-innovation—especially those aimed at addressing perceived "woke" or politically biased content in generative AI models[33].

[31] See *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) summer, in Bocconi Legal Studies Research Paper, 2025, SSRN: <https://ssrn.com/abstract=5302544>.

[32] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

[33] U.S. House of Representatives, Censorship's Next Frontier: The Federal Government's Attempt to Control Artificial Intelligence to Suppress Free Speech, Interim Staff Report of the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government U.S. House of Representatives, December 18, 2024.

4. On the Future Possible Circulation of the EU Legal Model

In recent decades, we have witnessed a profound transformation in the role of law (particularly private law) within the legal system, marked by a gradual loss of its centrality in favor of regulatory law and technical rules. This shift reflects not only an evolution in the forms of norm production but also a change in the very conception of law, increasingly seen as a functional tool for the economy rather than as an expression of general and structural principles intended to endure over time.

Classical private law, grounded in the 19th-century civil code model, was based on abstract, stable, and flexible categories designed to ensure legal certainty and to regulate interpersonal relationships in a systematic logic. However, in contemporary times, this framework has been progressively overshadowed by regulatory law—understood as a set of sector-specific rules, often of a public law nature, aimed at regulating specific areas of the economy (e.g., energy, telecommunications, finance, healthcare, environment) through targeted, contingent, and often technocratic interventions.

As leading scholars have observed, "private law has given way to a functional type of law, governed by independent authorities and efficiency logics, often disconnected from any systemic design." [34] These results in a form of "episodic" legislation, where overall coherence is sacrificed on the altar of political urgency, market pressure, or media contingencies. Legislators abandon the construction of durable, structural norms in favor of producing legal texts designed to address immediate problems, without any long-term vision.

Regulatory law represents the triumph of *governance by instruments*—as sharply noted—a form of public policy implemented through technical tools, bypassing political deliberation and democratic debate[35]. In this process, law tends to lose its ordering and predictive function, becoming a patchwork of special, heterogeneous rules lacking any systemic vision. The AI Act—despite laying down certain principles—is a prime example: a complex tangle of sectoral rules, often considered ill-suited even by technical experts and difficult to understand (and apply) for legal professionals.

In this context, the normative language itself is affected by the technocratic drift: norms are often written in hyper-detailed form, with continuous references to implementing regulations or technical standards, making them hard to understand not only for the average citizen but also for legal practitioners. This creates a deficit in accessibility and a disconnect between the law and its recipients, undermining the principle of substantive legality. A paradigmatic example is definition no. 67 in Article 3 of the AI Act, which defines "floating point operation" as "any mathematical operation or assignment involving floating point numbers, a subset of real numbers

[34] *Alpa G.,* Diritto privato e tecnica legislativa, 2018, see also *Micklitz H. W.,* Introduction, in Costitutionalization of European Private Law, Oxford, 2014, 1.
[35] *Lascoumes P., Le Gales P.* (éds.), Gouverner par les instruments, Science Po, Paris, 2005.

generally represented on computers using a fixed-precision integer with a scaling factor that is an integer exponent of a fixed base."

Some scholars have linked this transformation to the rise of the neoliberal paradigm, which has produced a vision of law as a technical instrument in the service of the market rather than as a vehicle for justice or social rebalancing—where the supposed "technical neutrality" of law is a myth: every regulatory choice affects power structures and reflects specific interests, and thus corresponds to a selection of which interests are to be protected over others[36].

However, this is not the only reason for the waning of the *Brussels Effect*. Another cause is the legislative "flood": Digital Services Act, Digital Markets Act, Artificial Intelligence Act, Cyber Resilience Act, Data Act, Data Governance Act—just to name a few. This massive production, often labeled as soft law but in practice binding, comes from administrative authorities both at the central and national levels. It exacerbates the risk of inconsistencies among legal texts, which are frequently the result of lobbying pressures and therefore poorly coordinated within a unified and coherent legislative vision[37].

This overproduction of norms, not matched by an equally robust technological development at the European level, creates paradoxical effects (e.g., the companies subjected to the first bans under Article 5 of the AI Act, in force since February 2025, are non-European). It also leads to differentiated business strategies, such as those adopted by some U.S. companies that have decided not to offer AI services within the European Union[38].

Moreover, as noted in the *Draghi Report* presented to the European Commission in late 2024, Europe has failed to foster companies with adequate technological capacity (and therefore comparable to U.S. and Chinese "giants") [39]. This results in Europe's total dependency on third-party actors[40]—a gap further amplified by slow decision-making processes, formalistic obligations (which are, not coincidentally, leading to revisions of the GDPR, starting with the elimination of the record-keeping requirement for SMEs) [41], and a limited ability to replicate virtuous practices in smaller or less technologically advanced Member States.

---

[36] *Purdy J.S., Grewal D.S., Kapczynski A., Sabeel Rahman K.,* note 23, 1791.

[37] Cf. *Padeiro P. J.F.*, Lobbying in the European Union's AI Act: the role of lobbying by the big five tech companies on the Council of EU's legislative process, Instituto Universitario de Lisboa, October 2024, 44; *Woll C., Artigas J.*, Big Tech's influence in the EU: Lobbying and digital governance, 61 European Journal of Political Research, 2022, 384; *Rozgonyi K.,* Digital giants and EU regulation: The lobbying strategies of Meta in Brussels, 19 Journal of Information Technology & Politics, 2022, 463.

[38] This is the case, for instance, of Apple: *Montgomery B.,* Apple delays launch of AI-powered features in Europe, blaming EU rules, The Guardian, 21 June 2024. Sharp tensions also arose in connection with the temporary suspension ordered by the Italian Data Protection Authority against OpenAI, the company behind ChatGPT. For further analysis on this case, see *Diurni A., Riccio G.M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, in 9 The Italian Law Journal, 2023, 474.

[39] Cf. *Draghi M.,* The future of European competitiveness, European Commission, 2024.

[40] Some examples from the Draghi Report, including the one mentioned in the text of the article, had already been addressed, among others, by *Renda A.*, Beyond the Brussels Effect. Leveraging Digital Regulation for Strategic Autonomy, FEPS – Foundation for European Progressive Studies, Brussels, 2022.

[41] Press Agency, Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications, 9 July 2025.

In conclusion, it is difficult to predict whether the European Union will be able to remain a beacon for the protection of fundamental rights in the context of AI development.

Some signals seem to point toward a decline in this influence and in the willingness of non-European companies—not only American ones—to adapt to European solutions. Consider, for instance, the response of the Chinese companies managing the large language model known as *DeepSeek*, who failed to respond to the requests of the Italian Data Protection Authority, apart from claiming that European privacy regulations did not apply to their activities[42]. An absurd response—it seems evident that the lawyers representing the Chinese companies could not have been unaware of the GDPR's scope of application—but one that nonetheless reveals a declining attractiveness of the European market for non-European AI companies.

In addition, perhaps this is the question we should return to: the European Union makes the rules, but are we still sure that the "innovator" countries are interested in following them?

Bibliography:

1. *Almada M.*, *Petit N.,* the EU AI Act: A Medley of Product Safety and Fundamental Rights. European University Institute, RSCAS Working Paper 2023/59, 2023.
2. *Alpa G.,* Diritto privato e tecnica legislativa, 2018.
3. *Ancel M.*, Utilità e metodi Del diritto comparato. Italian translation by P. Stanzione. Camerino, 1974.
4. *Ascarelli T.,* Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952.
5. *Bradford A.*, The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020.
6. *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities 5: 1140, 2022
7. *Cannon R.,* The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway." Federal Communications Law Journal 49: 52, 1996.
8. *Costantinesco L.,* metodo comparative, Torino, 2000.
9. *Creemers R.,* China's Emerging Data Protection Framework, SSRN. https://ssrn.com/abstract=3964684, 2021.
10. *Creemers R., Webster G.,* (trans.), Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina, 2021.

[42] Garante per la protezione dei dati personali, Provv. January 30, 2025, doc. web n. 10098477.

https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

11. *Diurni A., Riccio, G. M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, The Italian Law Journal 9: 474, 2023.
12. *Downes L.,* The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009.
13. *Draghi M.,* the Future of European Competitiveness. European Commission, 2024.
14. *Ferrajoli L.,* "Crisi del diritto e dei diritti nell'età della globalizzazione." Questione Giustizia. <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>, 2023.
15. *Geiger C., Frosio, G., Izyumenko E.,* the Oxford Handbook of Online Intermediary Liability. Oxford University Press, 2020.
16. *Gorla G.,* "Diritto comparato." Enciclopedia del diritto, XII, Milano, 1964.
17. *Grossi P.,* Aspetti giuridici della globalizzazione economica. In Atti della Accademia dei Georgofili, 2013.
18. *Hoecke M. Van*, ed. Epistemology and Methodology of Comparative Law. Hart Publishing, 2004.
19. *Imm M. R.,* Marketing Pornography on the Information Superhighway, Georgetown Law Journal 83: 1849, 1985.
20. *Kennedy D.,* Law-and-Economics from the Perspective of Critical Legal Studies. In The New Palgrave Dictionary of Economics and the Law, ed. *Newman P.,* London, <https://duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>, 2002.
21. *Lascoumes P*., *Le Galès P*., eds. Gouverner par les instruments. Sciences Po, Paris, 2005.
22. *Liz dos Santos A. L.,* Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. Revista dos Tribunais 105, 2020.
23. *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in the Artificial Intelligence (AI) summer, Bocconi Legal Studies Research Paper. SSRN: https://ssrn.com/abstract=5302544, 2025.
24. *Major A. M.,* Internet Red Light District: A Domain Name Proposal for Regulatory Zoning of Obscene Content, Marshall Journal of Computer & Information Law 21, 1997.
25. *Mattei U.,* Comparative Law and Economics. University of Michigan Press, 1997.
26. *Meier P., Métille S.,* Loi fédérale sur la protection des données. Helbing Lichtenhahn Verlag, 2023.
27. *Montgomery B.,* Apple Delays Launch of AI-powered Features in Europe, Blaming EU Rules. The Guardian, June 21, 2024.
28. *Moriconi C.,* Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China. Nordic Journal of Law and Social Research 9: 248, 2019.
29. *Pereira J. F.,* Lobbying in the European Union's AI Act: The Role of Lobbying by the Big Five Tech Companies. Instituto Universitário de Lisboa, 2024.

30. *Purdy J. S., Grewal D. S., Kapczynski A., Rahman S., K.,* Building a Law-and-Political-Economy Framework, Yale Law Journal 129: 1784, 2020.
31. *Renda A.* 2022. Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy. Foundation for European Progressive Studies (FEPS), Brussels.
32. *Richards N.,* Why Privacy Matters. Oxford University Press, 2021.
33. *Rozgonyi K.,* Digital Giants and EU Regulation: The Lobbying Strategies of Meta in Brussels, Journal of Information Technology & Politics 19: 463, 2022.
34. *Sacco R.,* Circolazione e mutazione dei modelli giuridici, In Digesto delle discipline privatistiche, sez. civ., II. Torino: UTET, 365, 1988.
35. *Sacco R.,* Introduzione al diritto comparato. Fifth ed., in Trattato di diritto comparato, Torino: UTET, 1992.
36. *Santoni G*., Personal Data as a Market Commodity: Legal Irritants from China's Experience, European Journal of Privacy Law and Technology 1, 2023.
37. *Stanzione P.,* Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974.
38. United States Code, Title 18, Chapter 7, Title 47 § 223.
39. *Verbiest T., Spindler G., Riccio G. M.,* Study on the Liability of Internet Intermediaries. European Commission, DG Internal Market. SSRN: https://ssrn.com/abstract=2575069, 2002.
40. *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in Souza C.A., *Magrani E., Silva P.,* (eds.), Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.
41. *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.
42. *Woll C., Artigas, J.* Big Tech's Influence in the EU: Lobbying and Digital Governance. European Journal of Political Research 61: 384, 2022.
43. *Zeno-Zencovich V.,* Comparison Involves Pluralism: A Rejected Viewpoint, Comparative Law Review 6, 2025.
44. *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.