ESTUDIOS

LIQUID LAW AND THE CONSTITUTIONAL MULTIVERSE

GOVERNING GLOBALIZATION, DIGITALIZATION, AND JUSTICE BEYOND BORDERS

PERE SIMÓN CASTELLANO

ARANZADI

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Customer Service: https://areacliente.aranzadilaley.es

This work has been carried out within the framework of the research project *Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas* [2023-2025] (PID2022-13642OB-I00), funded by MCIN/AEI/10.13039/501100011033 and *FEDER Una manera de hacer Europa*. IP's: Lorenzo Cotino Hueso and Jorge Castellano Claramunt.

First edition: June 2025

Legal Deposit: M-14526-2025
ISBN print version: 978-84-1162-842-6
ISBN electronic version: 978-84-1162-843-3

Design, Prepress and Printing: ARANZADI LA LEY, S.A.U.
Printed in Spain

Índice General

Página

Chapter 4

The Disruption of Law in the Digital Age

The digital revolution has fundamentally altered the way society functions, how individuals interact with institutions, and, crucially, how law is conceptualized, created, and enforced. At the intersection of legal philosophy and practical governance, the digital transformation poses a direct challenge to the traditional structures and foundational principles of legal systems. These disruptions stem not only from the increasing reliance on data and algorithms to mediate decisions and societal interactions but also from the inadequacy of legal frameworks designed for an analog world in addressing the multifaceted realities of the digital age.

This part examines how the digital age disrupts the conceptual, structural, and operational dimensions of law, requiring a recalibration of its core functions. At the heart of this disruption lies the tension between two competing imperatives: the need for legal systems to uphold fundamental principles of justice, fairness, and accountability, and the rapid pace of technological innovation that often outstrips the capacity of these systems to respond effectively. The digital transformation thus raises profound questions: How can legal systems retain their coherence and legitimacy in the face of global, decentralized, and algorithm-driven forces? Is it possible to maintain the foundational ideals of the rule of law—predictability, accountability, and equality—in an era characterized by liquid law and fluid legal boundaries?

The evolving nature of rights in the digital era compels us to engage in a profound and critical reflection. One of the most striking features of the digital age is the emergence of new categories of rights that reflect the realities of a data-driven society. These include rights related to data protection, algorithmic transparency, freedom from automated discrimination, and even rights to digital existence and identity. These rights, which can be conceptualized as *über-rights* transcend the traditional boundaries of legal entitlements, addressing not only individual autonomy but also collective societal values such as equity, trust, and public welfare.

However, the evolution of rights in the digital age exposes significant tensions within classical legal doctrines. Traditional legal frameworks are deeply rooted in the positivist tradition, which emphasizes clearly defined rights, duties, and remedies. Yet the interconnected and globalized nature of digital systems defies this static conceptualization. For instance, the right to data protection under the GDPR reflects a sophisticated understanding of individual autonomy and informational self-determination. Still, it also demonstrates the limitations of existing legal structures in addressing collective harms, such as algorithmic biases or systemic inequalities perpetuated by data-driven systems.

Moreover, these new rights operate in a context where the distinction between private and public spheres is increasingly blurred. In the digital age, private entities wield immense power over public discourse, individual identities, and societal structures. This concentration of power challenges the state-centric model of legal regulation, necessitating innovative approaches to governance that account for the role of private actors as quasi-regulators and as subjects of regulation. Thus, the emergence of digital rights forces us to confront fundamental questions about the nature of law itself. Is law still an effective tool for ensuring justice in a world where power is mediated through algorithms and data flows rather than traditional institutions?

Another critical aspect of the disruption of law in the digital age is the fragmentation of legal authority. In a globalized world,

digital platforms and technologies operate across jurisdictions, creating complex regulatory challenges. National legal systems, designed to operate within defined territorial boundaries, struggle to address transnational issues such as data privacy, cybersecurity, and algorithmic accountability. This fragmentation is further exacerbated by the proliferation of overlapping and sometimes conflicting legal regimes at the local, national, and supranational levels.

The concept of multilevel constitutionalism offers a potential framework for navigating this complexity. By emphasizing the interconnectedness of legal systems at different levels, it seeks to harmonize conflicting norms and create a coherent legal order. However, this approach is not without its challenges. The rapid pace of technological innovation often outstrips the capacity of multilevel frameworks to adapt, leading to gaps in regulation and enforcement. Moreover, the plurality of legal actors—including states, international organizations, and private entities—complicates efforts to establish a unified legal framework.

This fragmentation has significant implications for the rule of law. The absence of a coherent regulatory framework undermines legal certainty and predictability, which are foundational to the legitimacy of legal systems. It also creates opportunities for regulatory arbitrage, where actors exploit differences between legal regimes to evade accountability. To address these challenges, legal systems must embrace a more dynamic and adaptive approach to governance, one that recognizes the fluid and interconnected nature of the digital world.

Perhaps the most immediate manifestation of the disruption of law in the digital age is the crisis of enforcement. Legal rights and protections are only meaningful if they can be effectively enforced. Yet the digital age exposes significant gaps in enforcement mechanisms, both at the individual and systemic levels.

At the individual level, enforcement often relies on affected parties to assert their rights through complaints or legal actions. This model

is ill-suited to the realities of the digital age, where harms are often diffuse, complex, and difficult to trace. For instance, algorithmic discrimination may affect millions of individuals in subtle and indirect ways, making it challenging to identify specific violations or assign responsibility. Moreover, the power asymmetry between individuals and large technology companies further undermines the effectiveness of traditional enforcement mechanisms.

At the systemic level, enforcement is hampered by a lack of resources, expertise, and coordination among regulatory authorities. Supervisory bodies, such as data protection authorities under the GDPR, often lack the capacity to address the scale and complexity of digital systems. This is particularly evident in the context of artificial intelligence, where the opacity and unpredictability of algorithmic decision-making pose unique challenges for oversight and accountability.

The limitations of traditional enforcement mechanisms underscore the need for innovative approaches to governance. One potential solution is the development of proactive regulatory frameworks that emphasize prevention and risk management rather than reactive enforcement. For example, regulatory sandboxes and impact assessments can provide mechanisms for identifying and mitigating risks before they result in harm. However, these approaches must be carefully designed to ensure that they do not compromise fundamental rights or create opportunities for regulatory capture.

The disruption of law in the digital age calls for a fundamental rethinking of legal and regulatory frameworks. To address the challenges of the digital age, legal systems must move beyond traditional models of regulation and embrace a more holistic approach that integrates legal, ethical, and technological perspectives.

Central to this holistic paradigm is the recognition of law as a dynamic and adaptive system. Rather than seeking to impose static rules on a rapidly changing world, legal systems must embrace flexibility and innovation. This requires a shift from rule-based regulation to

principle-based governance, where overarching principles such as fairness, accountability, and transparency guide the development and application of legal norms.

Moreover, a holistic regulatory paradigm must prioritize inclusivity and collaboration. The digital age affects all sectors of society, and addressing its challenges requires input from diverse stakeholders, including governments, businesses, civil society, and individuals. Interdisciplinary collaboration is particularly important, as many of the issues raised by digital technologies lie at the intersection of law, ethics, and technology. By fostering dialogue and cooperation among these fields, legal systems can develop more effective and equitable responses to the challenges of the digital age.

In this sense a holistic regulatory paradigm must recognize the importance of global governance. The interconnected nature of digital technologies requires coordinated action at the international level to address transnational issues such as data privacy, cybersecurity, and algorithmic accountability. This calls for the development of global norms and standards that reflect shared values and principles while respecting the diversity of legal and cultural contexts.

The disruption of law in the digital age represents both a profound challenge and an unprecedented opportunity. By embracing the complexities of the digital world and reimagining legal and regulatory frameworks, legal systems can not only address the challenges of the digital age but also reaffirm their role as arbiters of justice and protectors of fundamental rights. The subsequent sections delve deeper into specific aspects of this disruption, beginning with the critical issue of enforcement gaps and the disconnect between rights and remedies.

4.1. THE GAP BETWEEN RIGHTS AND REMEDIES

Digitalization has led to a proliferation of newly acknowledged rights, ranging from data protection and online privacy to the freedoms surrounding algorithmic transparency and content moderation.

At first glance, the expansion of these rights suggests an era where individuals are better protected than in previous decades, thanks to heightened awareness and a vibrant international dialogue about online harm, digital consumer protection, and emerging forms of discrimination. However, the modern reality reveals a critical divide between the recognition of such entitlements and the real-world mechanisms available to vindicate them. Legal scholars describe this as the chasm between rights and remedies, where a formal declaration of individual prerogatives does not necessarily translate into effective or timely enforcement.

One of the most pressing reasons for this gap lies in the inherently borderless nature of digital interactions.[1] Traditional legal doctrines, grounded in territorial sovereignty, struggle to keep pace with multinational platforms and decentralized networks that seamlessly operate across continents. Under a framework of liquid law, where legal norms become fluid and adaptive in response to new technological realities, there is an evident mismatch: norms evolve at different speeds, yet the remedies remain tied to jurisdictional boundaries. Individuals harmed by transnational data breaches or algorithmic errors often confront formidable hurdles when seeking redress.[2] Where does one file a claim? Which court has jurisdiction, and whose

1. The transnational flow of personal data renders traditional enforcement tools largely ineffective, as both governments and private entities can bypass jurisdictional constraints with ease. Unless regulatory bodies learn to collaborate across borders, these data streams will continue to undermine the ability of national laws to protect individuals. Transnational data governance thus becomes a key challenge for modern legal systems, as it not only tests their capacity to enforce rules but also questions the limits of national sovereignty in the digital age. See Radu, R. (2019). *Negotiating Internet Governance: Foreign Policy, Sovereignty, and Cyberspace*. Oxford University Press.
2. In a world marked by rapid shifts in technological paradigms, law must embrace an adaptable architecture that can respond to novel realities. Emphasizing rigidity in legal doctrines risks creating a temporal lag between societal changes and the formal recognition of rights. A fluid legal framework anticipates change, operating less like a static command and more like a dynamic system of guidelines that evolve alongside emerging social, economic, and technological conditions. See Teubner, G. (2012). *Constitutional Fragments: Societal Constitutionalism and Globalization*. Oxford University Press.

rules apply? The recognition that one has a right to online privacy, for example, may be acknowledged in multiple legal regimes, yet the enforcement pathways might differ drastically, creating confusion and obstructing timely relief.[3]

Moreover, the complexity of digital services exposes users to a myriad of potential harms not adequately addressed by traditional remedial mechanisms. Tech conglomerates process billions of data points each day. When something goes awry—whether it involves data misuse, identity theft, or algorithmic discrimination—affected individuals may find themselves negotiating with opaque corporate policies or labyrinthine dispute resolution systems. In this constitutional multiverse, where multiple legal orders overlap, it becomes increasingly unclear which normative framework prevails. A person might hold a data privacy right recognized under national legislation while also being entitled to broader protections spelled out in supranational agreements or regional charters. The multiplicity of norms does not guarantee a corresponding multiplicity of effective remedies. Instead, it may fracture the enforcement landscape and induce forum-shopping or, more commonly, discouragement from pursuing any remedy at all.

It is likewise instructive to look at how public authorities can, or cannot, respond to this enforcement challenge. States frequently operate under resource constraints, lacking specialized personnel with the technical expertise to investigate or litigate digital misconduct. Agencies established to police digital abuses, such as data protection authorities, sometimes face political pressures or budgetary

3. Without uniform procedures for cross-border redress, individuals are left navigating a maze of conflicting requirements. By the time a complaint is appropriately filed in one jurisdiction, evidence might be irretrievably lost, or the responsible entity may have shifted its operational base. Consequently, delays compound existing harms, forcing victims to endure a procedural limbo while corporations exploit loopholes in enforcement. Such fragmentation is arguably the greatest obstacle to bridging the gap between declared rights and actual remedies. See Koops, E. J. (2014). *Should ICT Regulation Be Technology-Neutral?* In B. van der Sloot, D. Broeders, & E. Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 77–98). Amsterdam University Press.

limitations.[4] The sheer velocity of technological evolution exacerbates this gap. Hackers, illicit data brokers, and unscrupulous application developers can outmaneuver regulators by rapidly relocating servers or masking network traffic. Consequently, the existence of robust rights in legislatures' statutes or judicial precedents does not necessarily align with equally robust avenues for accountability, restitution, or penalties.

Another factor fueling the gap is a societal shift in expectations. Users are encouraged to create content, share personal data, and rely on digital tools that mediate every aspect of daily life. They are promised safeguards, from end-to-end encryption to explicit opt-in consent frameworks. Yet when those promises fail—when data leaks occur, when automated systems yield biased results, or when online abuse escalates—users encounter significant difficulties in obtaining immediate and meaningful recourse. A question worth contemplating is whether the emphasis on enumerating digital rights has overshadowed the urgency of designing innovative and cross-border remedies. Can we continue to celebrate the proliferation of new rights without simultaneously advancing the institutional architecture that ensures real enforcement?

Multilevel constitutionalism offers a compelling lens to diagnose and address this systemic shortcoming. In a hyperconnected world,[5]

4. Regulatory capture is not only a theoretical concern but a real possibility when oversight bodies depend on government resources or face private sector lobbying. Ensuring genuine independence demands transparent funding structures, robust conflict-of-interest rules, and ongoing public scrutiny, lest the promise of impartial enforcement be hollowed out by external interests. See Carpenter, D., & Moss, D. A. (Eds.). (2014). *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*. Cambridge University Press.
5. In a hyperconnected environment, digital platforms function as global infrastructures that surpass the regulatory capacity of individual states. This shift towards supranational or network-based models of constitutionalism requires not only legislative coordination but also the development of new norms that secure public trust. When dealing with AI specifically, accountability is often blurred by algorithmic complexity and corporate secrecy, making a multilevel approach—where local, regional, and international bodies collaborate—vital

we see overlapping jurisdictions and competing legal orders. This structure may enable nuanced, context-specific norms, but it equally risks diluting the overall efficacy of legal protections. Achieving genuine accountability requires cooperation among national, regional, and transnational bodies. Mechanisms for joint investigations, extradition of digital offenders, and harmonized enforcement policies are crucial steps in bridging the divide between lofty aspirations and tangible results. Absent such coordination, unscrupulous actors exploit jurisdictional gray areas, while legitimate claimants face protracted legal battles that yield little practical relief.

Another salient dimension arises when considering the interplay between iusnaturalism and legal positivism in the digital context. Certain fundamental rights—such as dignity, autonomy, or freedom from discrimination—can be justified on natural law grounds, appealing to moral principles that transcend national frontiers. Yet the enforcement structures rely heavily on positivist frameworks: codified statutes, regulatory bodies, and courts bound by formal procedures. This philosophical tension becomes stark in matters like algorithmic decision-making. Claiming that an individual has a natural right to be free from opaque or prejudicial automated processes remains a normative aspiration unless legal systems produce binding regulations and accessible enforcement forums. The moral claim, however powerful, lacks practical impact if no tribunal is willing and able to hear the complaint and impose corrective measures.

Compounding the issue, private actors often regulate vast digital spaces. Internet service providers, social media companies, and e-commerce platforms wield quasi-governmental powers over user communities. They set terms of service, adjudicate alleged violations, and mete out punishments ranging from account suspensions to permanent bans. Some of these private entities impose internal review mechanisms or rely on specialized oversight boards. Nevertheless, the

---

for protecting rights and maintaining transparent governance. See Walker, N. (2018). *Intimations of Global Law*. Cambridge University Press.

legal enforceability of user rights within these corporate structures remains contingent on each platform's policies. Where a constitutional framework is lacking or weak, the private entity's internal rules dominate, undermining the uniformity and predictability that hallmark the rule of law. Although corporate self-regulation can provide quicker resolutions, it also raises questions. Do internal processes that lack transparency and formal legal safeguards truly remedy infringements of individuals' rights?

International organizations and civil society groups have begun to raise awareness of the need for more robust remedial frameworks. Multilateral treaties, cross-border enforcement compacts, and specialized digital courts are among the proposals floating in the evolving global legal discourse. Yet implementing such innovations presents its own challenges: sovereignty concerns, resource limitations, and disagreements regarding procedural standards can stall even the most promising initiatives. Some advocates suggest harnessing blockchain-based dispute resolution or other advanced technologies as a neutral means to bridge national boundaries. These experiments reflect the spirit of *liquid law*, which embraces flexible, tech-driven solutions. The question remains whether these platforms can reliably secure compliance and redress without replicating the pitfalls of existing systems.

Bridging the gap between rights and remedies in the digital domain demands a combination of legal reform, collaborative enforcement, and technological innovation. Adopting a purely national approach is inadequate, as digital life transcends borders. Equally, deferring entirely to global bodies or tech corporations risks diluting national sovereignty and democratic accountability. Achieving equilibrium in this constitutional multiverse requires sustained, coordinated efforts among stakeholders in governments, international organizations, the private sector, and user communities. The stakes could not be higher. If unaddressed, the gap between rights and remedies in the digital era threatens public trust in legal institutions and may diminish respect for the rule of law as a foundation of orderly coexistence.

The challenge, therefore, is to ensure that recognition of digital rights—whether anchored in moral claims or statutory frameworks—does not remain a mere aspiration. Individuals must possess viable paths to vindicate their entitlements before impartial and competent authorities. How can we best integrate emerging technologies with tried-and-tested procedural guarantees? And how do we preserve essential sovereignty while embracing transnational cooperation? Those are the pressing questions that confront policymakers and legal theorists striving to close the gap between rights and remedies in the digital age. Progress in this area will not only bolster the legitimacy of legal systems worldwide but also reaffirm the foundational ideals that undergird constitutional orders in an era of relentless technological change.

4.1.1. EVOLVING LEGAL FRAMEWORKS: FROM GDPR TO THE AI ACT

The trajectory of legal innovation in recent years demonstrates a determined effort to reconcile fast-paced technological growth with safeguards for individual autonomy, human dignity, and societal welfare. A pivotal development arose with the GDPR in the European Union. Regarded as one of the most comprehensive data protection regimes in the world, it has substantially influenced corporate strategies, international data flows, and the policies of tech giants. This framework, known for its extraterritorial reach and emphasis on user consent,[6] effectively recalibrated discussions surrounding

6. By establishing a principle of extraterritorial jurisdiction, the GDPR reshaped the global data protection landscape, compelling multinational enterprises to align with European standards. This strategy not only reaffirms the EU's normative power but also illuminates the complexities of enforcing compliance across multiple legal orders. Firms operating in different jurisdictions may face contradictory obligations, raising the specter of compliance fatigue and legal uncertainty. Nonetheless, the GDPR's robust enforcement mechanism, including hefty fines, demonstrates how a strategically designed regulation can influence corporate behavior far beyond its geographical origins. See Kuner, C. (2020). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

privacy and accountability in digital contexts. Nevertheless, the GDPR also illustrates the tension between legislative ambition and the practicability of enforcement, thereby echoing the gap between rights and remedies identified above.

An intriguing shift is occurring as lawmakers advance beyond data protection laws into regulating emerging technologies, particularly artificial intelligence. The proposed AI Act in the EU aims to establish a risk-based taxonomy of AI systems,[7] thereby tailoring regulatory obligations to the severity and likelihood of harm. Each iteration of this legislative process, however, reveals a fundamental question: is the law agile enough to address the complexities of machine learning models that evolve daily through self-training and global data harvesting? Under the umbrella of liquid law, traditional legislative cycles might struggle to keep pace with the quantum leaps in AI capabilities. Regulation, by its nature, seeks to define permissible conduct and ensure accountability. Yet the inherent dynamism of AI—where systems can autonomously generate novel functions—poses a formidable challenge to prescriptive statutes.

The EU's ambitions in this area are reshaping global conversations about ethical AI, algorithmic fairness, and the responsibilities of tech companies to ensure that automated decisions do not undermine fundamental liberties. The effort to export these standards beyond European borders—reminiscent of the GDPR's extraterritoriality—represents a fascinating aspect of multilevel constitutionalism in the digital sphere. Various jurisdictions are observing how these frameworks are playing out, eager to adopt similar measures or at

7. Framing AI regulation in terms of risk levels underscores the realization that a one-size-fits-all approach is inadequate in this rapidly developing field. By classifying systems based on their potential to harm individual rights or societal interests, legislators can craft targeted obligations proportionate to the AI application's impact. This not only fosters innovation where it is beneficial but also ensures a firmer grip on high-stakes deployments, such as facial recognition in public spaces or algorithmic credit scoring. See Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law & Security Review*, 43, 105506.

least adapt core principles to local contexts. Meanwhile, supranational entities and international organizations are grappling with harmonization of rules in a world where data respects no borders and multinational corporations often surpass the economic power of smaller states. This evolving situation accentuates the complexities of the constitutional multiverse and the necessity for broad stakeholder collaboration.

In the realm of enforcement, the GDPR and the prospective AI Act offer a portrait of how lawmakers attempt to bridge the divide between normative aspirations and actual remedies. The GDPR instituted heavy financial penalties for noncompliance, reflecting a strategic choice to deter corporate misconduct. National data protection authorities hold the power to investigate infringements and impose fines. This approach has led to several high-profile cases involving large tech corporations. Nonetheless, critics contend that such actions, while symbolically potent, do not always alter corporate practices. Financial penalties may be absorbed as a cost of doing business, particularly for entities with vast economic reserves. Similar issues are poised to emerge under the AI Act. Will imposing penalties suffice to ensure compliance, or should the law incorporate more systemic interventions, such as mandatory transparency audits and real-time oversight of high-risk AI systems?

Legislators within and beyond the EU are also wrestling with the interplay between innovation and regulation. Burdensome or overly prescriptive norms risk stifling technological progress. Innovation is critical for economic growth and can produce public benefits, including medical breakthroughs and enhanced disaster response systems. At the same time, lax or poorly enforced regulations might undermine personal freedoms, perpetuate discrimination, and entrench social inequities through biased AI outputs. Finding the delicate balance between these extremes has become a defining challenge of our era. This balancing act resonates with fundamental debates within legal philosophy. Positivists prioritize clear, codified rules that delineate permissible and impermissible conduct. Iusnaturalists emphasize the moral imperatives that must guide technology's deployment, such

as the principle that individuals should never be reduced to mere data points. The AI Act, with its risk-based orientation, arguably tries to unify these perspectives by specifying concrete standards while upholding normative ideals related to privacy, fairness, and human oversight.

The ripple effects of the GDPR and the AI Act do not stop at conventional civil or administrative litigation. In many instances, individuals rely on private arbitration or corporate-led dispute resolution processes to address alleged violations. This phenomenon is partly due to the swift, transnational character of digital commerce. Users sign platform agreements that preclude them from filing class actions in domestic courts, pushing them toward alternative forums. Some laud these private tribunals for their speed and specialized expertise. Yet there remains a pressing concern about transparency, impartiality, and the uniform protection of rights, especially when the rules differ across regions in a constitutional multiverse. How can lawmakers ensure that private dispute mechanisms align with the spirit and letter of critical regulations like GDPR and the AI Act?

Another frontier in this evolving landscape concerns the integration of compliance-by-design. Systems architects and software engineers are being asked to incorporate legal and ethical considerations at the inception of product development. The GDPR's principles of data protection by design and by default have influenced this thinking. The AI Act extends similar logic by insisting on robust documentation and transparency in AI development cycles. Yet the technical intricacies of advanced models make it arduous to predict how an AI system might behave once deployed at scale. If the law mandates transparent, explainable AI, software designers must reconfigure data pipelines, model architectures, and user interfaces to accommodate interpretability. Achieving this paradigm shift requires not only technical expertise but also a deep alignment of corporate culture with regulatory objectives.

The broader implications for global governance are equally significant. The EU's initiatives can serve as prototypes for other

jurisdictions. Policymakers worldwide observe whether these regulations meaningfully protect citizens while preserving a competitive digital marketplace. Many actors—national governments, regional blocs, and civil society networks—are seeking to emulate or critique the European model. This cross-pollination of regulatory strategies is an instance of multilevel constitutionalism in action, as it fuses rules emerging from distinct legal orders, each with its own democratic processes and cultural values. Will the AI Act ultimately spur a new generation of regulation that addresses hyperconnected supply chains, autonomous decision-making, and bio-digital convergence?

Closing the circle, this movement from GDPR to the AI Act underscores the incremental yet profound shift toward advanced legal frameworks that attempt to reconcile technology's transformative power with the highest aspirations of the rule of law. Achieving coherence in this environment demands collaboration among legislatures, courts, executive agencies, private corporations, and an engaged public. The era when national parliaments could legislate in splendid isolation is over. In a world marked by liquid law, regulators must embrace flexible, adaptive approaches, whether by leveraging cross-border information-sharing or building new institutional mechanisms dedicated to tech oversight.

Crucially, any legal regime, however sophisticated, will fall short if it fails to secure meaningful avenues of redress for aggrieved individuals or communities. Whether the focus is on data privacy under the GDPR or algorithmic accountability under the AI Act, enforcement must be robust, accessible, and consistent. Without tangible remedies, lofty proclamations ring hollow, and public trust in democratic governance erodes. Are legislators, regulators, and technology firms prepared to transcend vested interests and collaborate in forging innovative, enforceable solutions? That question lies at the heart of the contemporary endeavor to craft a digital legal order that remains steadfast to constitutional values while accommodating the relentless momentum of technological change.

4.1.2. CHALLENGES OF ENFORCEMENT: SUPERVISORY AUTHORITIES AND THEIR LIMITATIONS

Enforcement in the digital realm frequently relies on specialized supervisory bodies entrusted with monitoring compliance and punishing infringements. Yet many of these authorities operate under significant structural, legal, and resource-related constraints. Despite new regulatory frameworks lauded for their ambition and comprehensive scope, such as the GDPR, persistent challenges undermine their effectiveness in practice. These challenges reflect a broader tension between expansive legal provisions and the realities of day-to-day oversight, ultimately raising questions about the viability of existing enforcement mechanisms.

One core limitation stems from jurisdictional boundaries. Supervisory authorities typically hold power within a national or regional context, while digital platforms and data flows transcend borders with ease. This mismatch between global corporate activities and territorially confined agencies generates an enforcement gap. Even where reciprocal agreements exist among different regulators, complex questions about conflict of laws and overlapping mandates can cause delayed investigations and uneven sanctions.[8] Such fragmentation prompts debate about whether a more centralized, global approach is both necessary and feasible within the evolving constitutional multiverse.

Another challenge relates to the uneven distribution of resources. Many national-level authorities lack the funding, technical know-how, and human capital essential for robust oversight in domains

8. The divergence in sanctions across different legal systems creates a patchwork of enforcement outcomes. Some jurisdictions may impose minimal penalties, effectively incentivizing companies to operate there, while stricter regimes become less attractive business hubs. This asymmetry underscores the importance of mutual recognition of judgments and closer international cooperation to prevent forum-shopping and guarantee consistent remedies for rights violations. See Scott, J., & Sturm, S. (2007). Courts as Catalysts: Rethinking the Judicial Role in New Governance. *Columbia Journal of European Law*, 13(3), 565–594.

such as big data analytics or artificial intelligence. Corporate entities, in contrast, often command teams of specialists and considerable financial reserves. This imbalance hampers the ability of supervisory bodies to keep pace with technological developments. The very notion of liquid law underscores the need for agile and adaptive responses; yet authorities burdened by rigid bureaucratic procedures and limited resources struggle to adjust swiftly to novel forms of digital wrongdoing.[9]

Complexity also arises where national authorities must grapple with multinational corporations that operate under varied legal orders. Conflict-of-law principles, transnational immunity claims, and multiple layers of corporate ownership frequently obstruct or postpone enforcement. Meanwhile, each supervisory authority may approach violations differently. Some prioritize conciliatory methods—seeking compliance through negotiation—whereas others prefer imposing stringent fines. This divergence in approach feeds perceptions of inconsistency and fuels corporate attempts to exploit regulatory arbitrage. Do inconsistent enforcement styles risk erode public confidence in the system at large?

Another complication is the delicate balance between encouraging innovation and preventing digital abuses. Supervisory bodies are often tasked not merely with punishing infractions but also with supporting competitiveness, fostering market dynamism, and respecting national economic interests. Pressures from industry lobbyists or political stakeholders can dilute enforcement actions, making agencies cautious in imposing harsh penalties. When regulators temper enforcement for fear of stifling technological progress, the outcome can be a watered-

9. Even well-intentioned agencies can be hamstrung by the sheer scale of digital operations, which require sophisticated technical expertise and continuous monitoring. If regulators are to keep pace with major tech platforms, they must cultivate in-house competencies in data science and algorithmic auditing. Yet financial and political constraints persist, often resulting in regulatory bodies that cannot fulfill their mission of protecting consumer and citizen rights against the persistent onslaught of corporate influence. See Binns, R. (2018). Algorithmic Accountability and Public Reason. Philosophy & Technology, 31(4), 543–556.

down regimen of compliance that fails to safeguard fundamental rights effectively.

There is also the structural issue of democratic accountability. National parliaments or transnational entities entrust supervisory bodies with considerable power to interpret, investigate, and sanction under broad legislative mandates. Questions arise about legitimacy: how can these agencies be held accountable if their decisions produce substantial consequences for individual rights and corporate fortunes? If oversight boards and appeal mechanisms are weak, agencies risk both under- and over-enforcement, either shielding powerful entities from scrutiny or imposing disproportionate penalties. Striking the right balance between autonomy and accountability remains a key concern in a system that purports to uphold the rule of law.

Technological sophistication further complicates enforcement. Issues such as algorithmic transparency, biometric identification, and real-time data processing demand specialized technical insight. Supervisory authorities must rely on expert's adept at scrutinizing cryptographic protocols, machine-learning models, and complex data ecosystems. However, the pool of such experts is limited, and many prefer more lucrative positions in private industry. This shortage of skilled personnel leaves authorities ill-equipped to parse sophisticated violations, weakening their deterrent effect. Are we prepared to invest adequately in training, recruitment, and retention of technical specialists within public bodies?

Finally, the interplay of philosophical frameworks also shapes enforcement. Iusnaturalist views emphasize the inherent moral value of privacy and autonomy, while positivist norms direct agencies to follow codified law with meticulous neutrality. Reconciling these approaches in emergent areas—where normative guidance remains unsettled—presents a demanding task. Ambiguity in the legal and moral status of new technologies can paralyze enforcement agencies uncertain of how to interpret regulations in line with deeper constitutional values.

In sum, supervisory authorities face a suite of limitations that hamper their ability to ensure consistent, effective enforcement across the digital landscape. Jurisdictional fragmentation, limited resources, political pressures, and technical complexity all conspire to undercut the promise of robust oversight. Although new proposals and reforms aim to strengthen these agencies—through cross-border collaboration, enhanced funding, or specialized training—the fundamental question persists: can these incremental measures keep pace with the breathtaking speed of digital transformation? The future of global governance may depend on how effectively supervisory bodies adapt to these challenges while safeguarding both innovation and the fundamental rights essential to any democratic society.

4.1.3. RIGHTS WITHOUT TEETH: THE DISCONNECTION BETWEEN LEGAL PROVISIONS AND PRACTICAL TOOLS

New legal provisions in data protection, AI governance, and digital consumer protection often appear promising. They recognize expansive rights related to privacy, algorithmic fairness, content moderation, and more. The central dilemma, however, lies in ensuring that these rights are not merely symbolic but truly actionable. A proliferation of ambitious regulations does not automatically guarantee practical, accessible tools for individuals seeking remedies. This widening gulf is a pivotal concern in a constitutional multiverse where multiple jurisdictions, legal philosophies, and enforcement bodies intersect.

Enacted laws identify rights holders, detail procedural rules, and specify sanctions for breaches. Yet individuals frequently struggle to navigate bureaucratic processes, or even ascertain the correct forum for lodging complaints. Drafting statutory language is, in many respects, the simplest step in producing meaningful legal outcomes. Providing user-friendly dispute-resolution platforms, timely support from public institutions, and legal assistance to vulnerable parties

requires complex coordination.[10] Systems designed with an eye toward theoretical comprehensiveness can inadvertently neglect the complexities of everyday enforcement and user engagement.

Many jurisdictions now introduce digital rights, including portability or erasure of personal data. While these are lauded as milestones, the act of exercising them can be cumbersome. Corporate data controllers may bury relevant procedures in lengthy terms of service, respond slowly to user requests, or impose technical hurdles that dissuade individuals from pursuing their claims. Where official mechanisms exist for appeal, processing times can stretch indefinitely, undercutting the principle of swift redress. Additionally, compensation for infringements is notoriously difficult to calculate, especially if the harm involves intangible elements such as emotional distress or reputational damage. How can regulators and courts accurately value claims rooted in lost privacy or biased algorithmic outcomes?

Another cause of disconnection emerges from the inherent complexity of digital infrastructures. Automated systems that profile users or filter online content often do so through proprietary algorithms operating on immense datasets. Even if legislation grants users a *right to explanation*, unraveling the chain of logic in a deep-learning model can be daunting. Without robust interpretability tools, individuals cannot effectively assert their rights or challenge algorithmic decisions that affect their opportunities in areas like employment, lending, or social benefits. The notion of liquid law suggests the need for agile solutions, yet legal texts still tend toward static formulations that fail to incorporate dynamic technical safeguards.

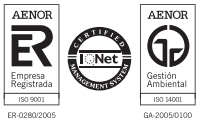
10. User-friendly digital platforms for lodging complaints or verifying compliance can substantially lower the barriers that prevent individuals from enforcing their rights. Yet building these tools requires a nuanced understanding of varying levels of digital literacy, as well as the linguistic and cultural diversity of users. A universal design approach, coupled with robust public support, ensures that even vulnerable or marginalized groups can navigate the complexities of digital legal procedures effectively and assert their entitlements. See Katsh, E., & Rabinovich-Einy, O. (2017). *Digital Justice: Technology and the Internet of Disputes.* Oxford University Press.

ESTUDIOS

Law in a liquid world defies the neat borders and entrenched hierarchies of the past. Globalization accelerates the fusion and friction of national systems, while digitalization amplifies corporate influence and spawns intangible conflicts that transcend territorial authority. In parallel, community justice movements reclaim local voices, yet pose formidable challenges of integration with universal rights. This book illuminates the intersection of these three transformative forces—mapping how constitutional law adapts, or fails to adapt, in an environment shaped by porous frontiers and algorithmic gatekeepers.

Drawing on concepts such as liquid law, multilevel constitutionalism, and über-rights, the author explains how legal frameworks both expand and fragment, offering novel solutions and revealing critical gaps. Traditional governance structures—built around nation-state exclusivity—confront digital platforms wielding near-sovereign powers, subcultures seeking recognition, and regulatory bodies struggling to harmonize universal entitlements with diverse cultural claims. The result is a dynamic interplay among transnational treaties, specialized agencies, and local dispute resolution, all guided by a vision of constitutional values robust enough to endure relentless technological change. This volume invites a rethinking of what law, sovereignty, and justice can mean in a fluid, global, and interconnected age.

ISBN: 978-84-1162-842-6



ARANZADI