International Journal of Economic Practices and Theories (IJEPT)
ISSN: 2247-7225
Volume 2026, Issue 1

Law and Society in the Digital Age: Legal Challenges and Social Transformation

[1]Gayatri Kapur, [2]Sulbha Goyal, [3]Ishita Khetarpal, [4]Mr. Gaurav Gupta, [5]Ms. Vrinda

[1]Assistant Professor, Bharati Vidyapeeth, Institute of Management and Research, New Delhi.

[2]Assistant Professor, Bharati Vidyapeeth, Institute of Management and Research, New Delhi.

[3]Lecturer, Jindal Global Law School, O.P Jindal Global University.

[4]Assistant Professor,Bharati Vidyapeeth, Institute of Management and Research, New Delhi.

[5]Phd Scholar, GD Goenka University.

Abstract

Classical foundations that underpin modern legal systems bounded territoriality, recognizable actors and a relatively stable technological base have been under threat from the swift spread of digital technologies, namely the internet, mobile devices, platform intermediaries and, most recently, artificial intelligence. This paper explores the connection between law and digital technology in the modern world on both sides; not only as the regulating institution in the context of technological change but also as an institution itself reshaped by technology. The paper outlines six main legal issues in the digital age data protection, cybercrime, artificial intelligence governance, platform regulation and intermediary liability, jurisdiction and digital sovereignty, and IP and four trends of socio-legal processes these map onto: digital inclusion, reorganization of work, public discourse, and reconstitution of identity, community online. The paper will utilize recent regional figures on the internet's penetration, overall costs of cybercrime and a comparison of the timelines of the different regulations in the region to suggest that economies in this region end up in a unique position: Asia-Pacific has the largest online population in the world, and their regulation in the digital world is far from even. The paper ends with policy recommendations to move towards a more responsive, proportional and regionally coordinated legal structure for digital governance.

Keywords: law and technology; digital governance; data protection; artificial intelligence regulation; cybercrime; socio-legal change; Asia-Pacific.

1. Introduction

Modern legal systems are constructed for a world of limited geographic scope, manifested actors, and modest change in technology. The word jurisdiction took on the aspect of a border, the word evidence the form of a document, and the word contract the form of a signature to be effected by someone who could be reached. None of these categories has been rendered redundant by digital technology, but each is now so wide-ranging that classical-doctrinal approaches to it alone do not find much confidence. A transaction may now start in a country, run on a server in another country and be sensed by a consumer in a third country within milliseconds; without any of the three jurisdictions on-site designating a rule for exactly this chain of actions.

This paper analyses “law and society in the digital age” as a truly bi-directional phenomenon and not as the foot race of technology traversing law behind which legislators must rush to keep. Digital technology, on the one hand, leads to novel legal issues digital harms (data breaches, algorithmic discrimination, non-consensual synthetic content), digital power dynamics (between states and platforms, between employers and gig workers, between traditional publishers and generative-AI-assisted creators) and the tension between inherited doctrinal concepts and digital technology (personhood, territory, publication, authorship). On its other side, law is a social institution, and digital technology changes the social circumstances within which law works: who petition the courts, who has a voice in public debate, how communities are formed and dissolved, and what becomes of that ‘public' which law addresses? Indeed, in this context it can be said that legal challenge and social transformation are two different ways of seeing the same phenomenon.

This relationship, the paper brings out through Asia-Pacific region, in particular for two reasons. First, the region is a genuinely global bellwether: it is simultaneously the world's largest online population and one of the least evenly connected, so that questions of digital rights inevitably run into questions of digital access. Second, the past three years have seen an unusually concentrated burst of regulatory activity across the region and its major trading partners; India's Digital Personal Data Protection Act, 2023 and its 2025 implementing rules, the European Union's Artificial Intelligence Act and its 2026 amendments, and Australia's world-first minimum age law for social media accounts, among others; that makes this an opportune moment to take stock.

2. Theoretical Framework: Reading Law and Technology Together

Classical legal positivism treats law as an external, sovereign-backed command directed at technology and its users: a legislature identifies harm and enacts a prohibition or permission. This picture is not wrong as much as incomplete. Lessig's (2006) account of four "modalities of regulation" law, social norms, markets and architecture remains the most economical corrective. For example, a platform's default privacy setting, an app's age-verification gate, or a smart contract's automated triggering are all forms of digital architecture, or "code," that regulate behaviour effectively and without giving courts a say. Even when code and law are different, code seems to ultimately prevail, as they are always at work, and don't need to be invoked or enforced separately. This is important to the present paper because many of the legal arguments outlined in Section 3 are, at their core, struggles over the code governing the actual use of the machine that actually govern conduct, whether that's a state-run code of conduct or a firm run code of conduct or some negotiated version of either.

The second element of the framework comes from Castells' (1996) network-society thesis. Castells does not believe digital technology merely adds new entities to the law's sphere of regulation; it remodels the notional "space of flows" of capital, information and images upon which social and economic life depends, and which was the focus of much legal doctrine, displacing it by the "space of places." Inevitably, a contract law which is based on the place of contract, or a defamation law built on the place of publication, is put under stress where the relevant action has no location whatsoever. These restructuring happen at a different pace from typical legislative and judicial action, generating what some have termed the "pacing problem" the time lapse between the start of the social impact of a technology and the development of a stable legal framework for it. From the inside, a solution to the pacing problem can be discerned in the European Union's own AI Act, which will enter into force internationally one of the most ambitious anticipatory technology regulations to date: two years after its adoption, the standards and infrastructure required for the assessment of the AI systems designated as high-risk in the AI Act still have not been finalized and the Act has had to be amended to allow for the postponement of the assessments (Gibson Dunn, 2026; European Commission, 2026).

A third, complementary account, is Teubner's (1993) systems-theoretic interpretation of law as an operationally self-referential "autopoietic" system, which not only cannot absorb disturbances directly from the outside of the economy or the outside of technology, but is in fact not faced with contradictory impulses of this kind. This is reflected in a recurring tendency in the content discussed below: legal reactions to digital technology are not necessarily a direct transposition of a technical or social issue but merely partial translations always accompanied by a remainder. Data protection law reframes the abstract and ubiquitous nature of "pervasive tracking" and restates the problem in the relatively dense language of "consent" and "purpose limitation" and "data fiduciary obligations," and platform law reframes the issue of "algorithmically amplified speech" and recasts it in the relatively dense language of "due diligence" and "intermediary liability." One reason why the very same issues re-emerge in slightly different guise a couple of years later is that none of the translation is ever finished it is that the translation is required or often valuable, but it is never complete.

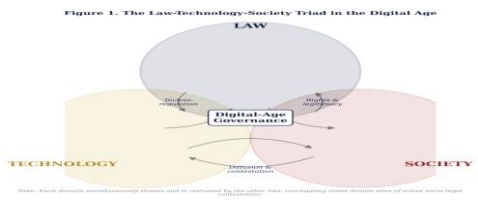

Figure 1. The Law-Technology-Society Triad in the Digital Age. Source: author's construction, drawing on Lessig (2006), Castells (1996) and Teubner (1993).

These three accounts are presented as triad in Figure 1. Likewise, although there is a sense of "regulator-regulated", law, technology and society continually shape each other, and the overlapping parts in this diagram correspond to the two parts of this paper: The "techno-regulation" overlap is more the legal challenge that is found in Section 3, while the "diffusion and contestation" space, where technology meets the texture of everyday social life is more what is found in Section 4, "the right to and legitimacy around technologies", with their age of consent and chief operation.

3. Mapping the Legal Challenges of the Digital Age

3.1 Privacy and data protection as the first frontier

Data protection has become the paradigm case of digital-age lawmaking because it was the first domain in which most jurisdictions confronted the problem squarely. India's trajectory is illustrative of a broader regional pattern. Before 2023, data protection in India rested on the thin foundation of the Information Technology Act, 2000 and the 2011 "Reasonable Security Practices" Rules made under it a regime designed principally for e-commerce and cybersecurity rather than comprehensive data governance. In the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, a nine judge panel of the Supreme Court of India concluded that the right to privacy is a fundamental right under Article 21 of the Constitution, thus the constitutional push for a law. This time it is the Digital Personal Data Protection Act, 2023 and the implementing rules were notified only in November 2025 over two years after the Hon'ble President had given assent to the Act a case of the pacing issue mentioned in Section 2. The Rules also take effect in a staggered manner: rule making by the Data Protection Board of India (DPBobI) takes effect on notification; obligations for consent managers take effect from 2026/11; and the major part of the obligations for data fiduciaries becomes effective from 2027/05 (Lexology, 2025; Fisher Phillips, 2026).

The DPDP Act is similar to the European Union's GDPR in some important aspects that impact its structure, such as its extraterritorial reach, its focus on individual rights of access, correction and erasure and its enforcement regimes, however there are also key differences: most significantly - greater exemptions for government processing, but also in a softer, more consensus oriented, formulation of purpose limitation (DLA Piper, 2026). Over the last decade or so, similar legislation has been adopted in the broader region: the Personal Data Protection Act, 2012 of Singapore, the Personal Information Protection Law of China (which comes into effect from November 2021), and a series of amendments to the Act on the Protection of Personal Information in Japan. There has consequently been a true legal change in Asia-Pacific data protection law from a set of sectoral rules to something closer to comprehensive territory coverage a change spanned across one lawmaking generation.

3.2 Cybercrime, cybersecurity and the limits of territorial law

The mismatch between the space of the criminal law and the space of the criminal activity it addresses is explicated through the cybercrime phenomenon. Investigation and prosecution remains significantly complementary to physical evidence, all memorialized by convention and practice in mutual legal assistance treaties and letters rogatory that can takes months to be executed, while the criminal activity increasingly takes the form of "cybercrime-as-a-service," including the use of AI to guide and craft phishing attacks and fraud, and such activity can be reconfigured in hours. If the Council of Europe's Budapest Convention on Cybercrime (2001) was multilateral harmonization of substantive and procedural laws on cybercrime, the other big economies in the region, i.e. India and China, were not States parties to the Convention, meaning that its reach is restricted where the case load is greatest.

Although it is hard to quantify exactly, the economic magnitude of the issue is huge, on any estimates. Other methodologies looking more directly at "reported losses" from cybercrime produce estimates as low as a factor of 10 less, as the note in Figure 3 makes clear; widely referenced industry projections put the total global cost of cybercrime at approximately US$10.5 trillion by 2025 and US$10.8 trillion by 2026, increasing to US$15.6 trillion by 2029 (Cybersecurity Ventures, 2026). One thing is not in dispute: Over the last decade, the costs of cybercrime have been rising significantly faster than global GDP, transforming what used to be considered primarily a technical security problem into a first-order issue for economic policy and, increasingly, civil law, as courts face up to facets of cybercrime such as harassment, extortion, and reputational injury (Citron, 2014).

3.3 Artificial intelligence and the problem of regulating a moving target

Artificial intelligence governance is at present the clearest illustration of the pacing problem introduced in Section 2. The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) widely described as the first comprehensive, economy-wide AI statute of its kind entered into force in August 2024, with its prohibitions on unacceptable-risk systems and AI-literacy obligations applying from February 2025 and its rules for general-purpose AI models from August 2025. By late 2025, however, implementation was visibly behind schedule, and the "Digital Omnibus on AI," politically agreed in May 2026, deferred the Act's central high-risk-system obligations by roughly sixteen months — from August 2026 to December 2027 for most use-based systems, and to August 2028 for AI embedded in regulated products (Gibson Dunn, 2026; European Commission, 2026). The same amendment added a new prohibition, effective from December 2026, on AI systems that generate non-consensual intimate imagery or child sexual abuse material, illustrating how anticipatory legislation is repeatedly supplemented in response to harms that were not fully visible at the time of drafting (Inside Privacy, 2026).

In contrast, India has yet to enact a standalone AI law and instead intends to adopt a regulatory-light approach grounded in sector-specific regulations and guidance within a framework of the existing IT Act, leaving China's targeted regulations for recommendation algorithms and generative content to cut deeper into the AI sector. The overall regional picture is one of not mere convergence around a single regulatory model, but of true regulatory divergence, resulting in compliance complexity for the firms operating across borders and a question as to whether any level of regional regulatory coordination is feasible, addressed in Section 6.

3.4 Platform governance, intermediary liability and speech

The governance of online platforms sits at the intersection of speech regulation and competition policy, and it is here that the "code as law" thesis introduced in Section 2 is most visible: platforms' terms of service, recommendation algorithms and content-moderation systems now do much of the practical work that speech law used to do through courts. Balkin (2018) captures this shift by describing contemporary speech governance as a "triangle" running between the state, speakers and platforms, rather than the traditional bilateral relationship between the state and the speaker that classical free-expression doctrine assumes; platforms exercise what he terms "new-school" speech regulation that is privately administered and only loosely accountable to public law.

India's experience illustrates both sides of this triangle. In Shreya Singhal v. Union of India (2015) 5 SCC 1, the Supreme Court struck down section 66A of the IT Act as unconstitutionally vague and overbroad, and read down intermediaries' liability under section 79 to require actual knowledge communicated through a court or government order a judgment generally read as protective of online expression. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 subsequently reintroduced significant due-diligence and traceability obligations on "significant social media intermediaries," and a since-invalidated 2023 amendment empowering a government "Fact Check Unit" to flag online content relating to government business as false was struck down by the Bombay High Court as an unconstitutional restriction on speech a reminder that the judiciary continues to check the state's own attempts to regulate platform content, not only the platforms themselves. The European Union's Digital Services Act (Regulation (EU) 2022/2065) takes a structurally different approach, imposing graduated systemic-risk-mitigation duties on the largest platforms rather than case-by-case content rules, offering a comparative model that several Asia-Pacific regulators are now studying.

3.5 Jurisdiction, data localization and digital sovereignty

Classical jurisdictional doctrine assumes that the relevant conduct, actor or effect can be located within a territory. Cloud computing and distributed data processing strain this assumption directly, since the same dataset may be replicated, processed and accessed across several jurisdictions simultaneously. States have acted on a continuum between soft coordination and hard localization. On the "light side," the Cross-Border Privacy Rules system of the Asia-Pacific Economic Cooperation forum is a voluntary certification system in which participating businesses can participate. On the tough end, the Personal Information Protection Law of the Republic of China mandates an assessment of security measures prior to moving certain types of data out of the country while India's DPDP Act, 2023 allows the government to notify a restriction on transfers to certain

jurisdictions.An influential criticism of this westering to “data nationalism” can be found in Chander and Le (2015), who find that localisation requirements involve substantial compliance and infrastructure burdens for firms, that are disproportionately imposed on smaller firms and are ultimately passed through to consumers as the recipient of the benefits, but that do not appreciably enhance security or the benefits to law enforcement, as a consequence of data storage locally does not make it impossible for the data to be breached or misused. This is, perhaps, the most obvious example in which, for a journal devoted to the economics of the Asia-Pacific region more specifically, legal doctrine and economic policy cannot be separated: localisation is legal, industrial policy and digital sovereignty all together, and its net welfare effect hinges upon empirical factors that are beyond the realm of legal analysis, including but not limited to compliance costs, market concentration and security outcomes.

3.6 Intellectual property in the digital economy

Another way that digital technology has shaken intellectual property doctrine is still being shaken out. Reference may be made very briefly to three trends. One reason is the legal disputes and legislative scrutiny that began in a variety of jurisdictions over the use of copyrighted work as training data for generative AI systems, stretching the old "fair use" and "fair dealing" legal concepts that were not originally conceived for use in the context of machine-learning training pipelines. Second, with the size of e-commerce platforms the problem is not only one of enforcement, but one of platform-governance as well, because the issue is how quickly listings of products infringing the trademark can be taken down from a marketplace. Third, data-driven innovation has shifted competitive advantage in many industries away from patentable inventions and toward trade secrets and proprietary datasets, which are harder to protect through registration-based IP regimes and have driven renewed interest in trade-secret and data-governance law as complements to classical intellectual property.

4. Social Transformation in the Digital Age

4.1 The digital divide and the limits of universal digital rights

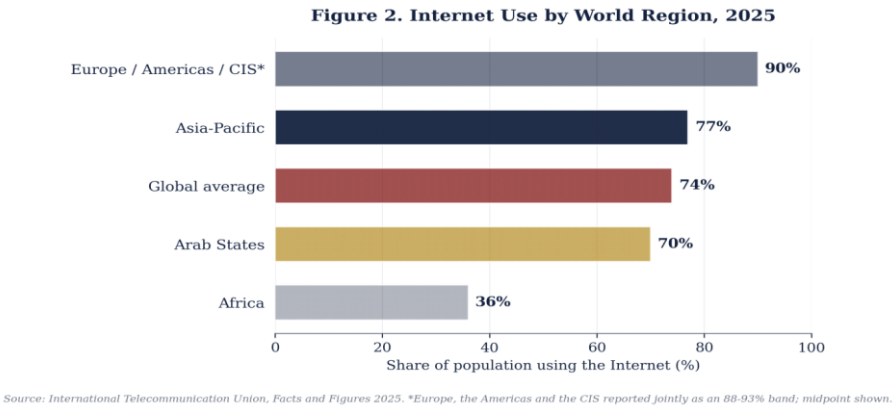

Figure 2. Internet use by world region, 2025. Source: International Telecommunication Union (2025).

Legal frameworks increasingly assume a baseline of digital access that a meaningful share of the region’s population does not yet have. Internet use in Asia and the Pacific stood at roughly 77 per cent of the population in 2025 broadly comparable to the global average of 74 per cent but well below the 88-93 per cent band typical of Europe, the Americas and the Commonwealth of Independent States (International Telecommunication Union, 2025; see Figure 2). Within the region, the gap is also gendered: 68 per cent of men in Asia and the Pacific were online in 2024 against 64 per cent of women, a gender-parity score of 0.95 that, while a substantial improvement from 0.89 five years earlier, still represents millions of women without meaningful digital access (ITU, 2025). A statutory right to data portability, or a right to be forgotten, means little to someone without a smartphone or reliable connectivity in the first place; digital-rights law of this kind is, in an important sense, written for the already-connected, and its practical reach is bounded by the access gap Figure 2 makes visible.

4.2 Platform work and the reconfiguration of labour

The platform economy has reorganized significant parts of the labour market around task-based, algorithmically managed work that does not map cleanly onto the employee/independent-contractor binary most labour law was built around. Jurisdictions have responded in different ways. In Uber BV v Aslam [2021] UKSC the Supreme Court of the United Kingdom again held that Uber drivers were "worker" as defined by the legislation, despite being character as independent contractors under the terms of their contracts. Taking an intermediate path, the Code on Social Security, 2020 introduces three statutorily defined categories of "gig worker", "platform worker" and "formal worker", providing welfare measures to "gig worker" and "platform worker", but not the status of formal workers. Both are part adaptations of an entirely new form of economic organisation to traditional legal categories, in Teubner's conception, and neither approach lays the tension between their flexibility and platforms and many workers and the social-protection floor that labour law traditionally guarantees to workers entirely.

4.3 Public discourse, misinformation and democratic participation

The algorithmically managed 'feed' has transformed the way in which public discourse is constructed in ways which legal doctrine, operating with a relatively narrower number of publishers did not expect. Sunstein (2017) and Benkler, Faris and Roberts (2018) characterize a media environment where personalised curation can undermine common factual bases even while providing increased raw data resources for information. Attempts to empower an 'independent' 'Fact Check Unit' run by the government as India did in 2023 have been contested and limited via the judiciary; similarly, the European Union's Digital Services Act provides for VLPs to analyse and address 'systemic risks' of disinformation, but the decision to label these as fact or fiction rests elsewhere. The comparison indicates that there is apparently a growing consensus, at least in the jurisdictions reviewed in this Casebook, that process-based obligations in relation to transparency, risk assessment, appeal mechanisms are more future-proof regulatory tools than direct state adjudication of the truth.

4.4 Identity, community and the networked self

As Cohen (2012) outlines, today's conception of "self" is more than just represented on these platforms; it is "networked" constituted by such platforms that dictate what information is presented to a person, who else can be found, and what a person's past "behaviors" are or are not. The implications for this have only just started to be addressed by legal frameworks that are still mostly in their infancy, especially as they concern children and adolescents for whom social experiences are mediated by platforms which are more largely conceived with tweets and 'Like' buttons in mind. The Online Safety Amendment (Social Media Minimum Age) Act 2024 requiring reasonably practicable measures to be implemented by designated platforms to prevent Australians under 16 years of age from holding accounts is the most sweeping legislative measure to date, and has garnered international as well as domestic interest as an experiment in limiting access to platforms based on age, with some other jurisdictions reportedly considering similar frameworks (eSafety Commissioner, 2026; Kennedys Law, 2026). The law, for what it is, is a clear case in point of the central assertion of Section 2: Social transformation in the process of online construction of identity and community produces a legal response one that, as it currently stands, is still experimental and contested.

5. Conclusion

Delhi is a city where Law and society have been in a true mutually beneficial relationship. Exhibited legal categories are required to be translated repetitively into digital technology, where this doctrine faces legal challenges regarding data protection, cybercrime, artificial intelligence, platform governance, jurisdiction and IP rights that in their essence can be solved only by translating into exhibited categories; and that translation is revisited in a few years after its first attempt. Meanwhile the social context or ground from which the law emerges is undergoing its own transformation at the hands of digital technology: connection, work, public discourse, identity and community. The Asia-Pacific region is unique in this situation, as it is home to the world's largest online population, has some of the least even connectivity and among the most actively evolving regulatory landscapes. Looking at the evidence here, it seems that the legal systems in this region have not just been behind the curve on technological change, nor necessarily just been catching up, but have been in an

ongoing, visible iterative mode of translation: a mode of lawmaking, this paper has implied, that is likely to stay a permanent feature rather than a transition to be outgrown in the digital age.

References

Legislation and Official Instruments

[1] Budapest Convention on Cybercrime, ETS No. 185 (Council of Europe, 2001).
[2] Code on Social Security, 2020 (India).
[3] Digital Personal Data Protection Act, 2023 (India).
[4] Digital Personal Data Protection Rules, 2025 (India), notified 13 November 2025.
[5] General Data Protection Regulation, Regulation (EU) 2016/679.
[6] Information Technology Act, 2000 (India).
[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[8] Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth, Australia).
[9] Personal Data Protection Act 2012 (Singapore).
[10] Personal Information Protection Law of the People's Republic of China (2021).
[11] Regulation (EU) 2022/2065 (Digital Services Act).
[12] Regulation (EU) 2024/1689 (Artificial Intelligence Act).
[13] Cases
[14] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India).
[15] Shreya Singhal v. Union of India (2015) 5 SCC 1 (Supreme Court of India).
[16] Uber BV v Aslam [2021] UKSC 5 (Supreme Court of the United Kingdom).

Books, Articles and Reports

[1] Balkin, J.M. (2018). Free speech is a triangle. Columbia Law Review, 118(7), 2011–2056.
[2] Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press.
[3] Benkler, Y., Faris, R., & Roberts, H. (2018). Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press.
[4] Castells, M. (1996). The Rise of the Network Society. Blackwell.
[5] Chander, A., & Le, U.P. (2015). Data nationalism. Emory Law Journal, 64(3), 677–739.
[6] Citron, D.K. (2014). Hate Crimes in Cyberspace. Harvard University Press.
[7] Cohen, J.E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press.
[8] Cybersecurity Ventures (2026). Official Cybercrime Report. Retrieved from cybersecurityventures.com.
[9] DLA Piper (2026). Data Protection Laws of the World: India. Retrieved from dlapiperdataprotection.com.
[10] eSafety Commissioner (2026). Social media age restrictions. Australian Government. Retrieved from esafety.gov.au.
[11] European Commission (2026). AI Act — Shaping Europe's Digital Future. Retrieved from digital-strategy.ec.europa.eu.
[12] Fisher Phillips (2026). India's New Data Privacy Rules Are Here: 8 Steps for Businesses. Retrieved from fisherphillips.com.
[13] Gibson Dunn (2026). EU AI Act Omnibus Agreement — Postponed High-Risk Deadlines and Other Key Changes. Retrieved from gibsondunn.com.
[14] Inside Privacy / Covington (2026). EU AI Act Update: Timeline Relief, Targeted Simplification, and New Prohibitions. Retrieved from insideprivacy.com.
[15] International Telecommunication Union (2025). State of Digital Development and Trends in Asia and the Pacific. ITU.
[16] Kennedys Law (2026). Australia's Social Media Ban for under 16s. Retrieved from kennedyslaw.com.
[17] Lessig, L. (2006). Code: Version 2.0. Basic Books.

[18] Lexology / S&R Associates (2025). India's Digital Personal Data Protection Regime Takes Effect. Retrieved from lexology.com.
[19] Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
[20] Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.
[21] Solove, D.J. (2008). Understanding Privacy. Harvard University Press.
[22] Sunstein, C.R. (2017). #Republic: Divided Democracy in the Age of Social Media. Princeton University Press.
[23] Susskind, R. (2019). Online Courts and the Future of Justice. Oxford University Press.
[24] Teubner, G. (1993). Law as an Autopoietic System. Blackwell.
[25] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the Frontier of Power. PublicAffairs.