JLP JOURNAL OF LAW AND POLITICS

Artificial Intelligence & The Violation of Right to Privacy Under Article 17 of the ICCPR

Md. Arif Rayhan

©Author(s)

DOI: https://doi.org//10.69648/CUYL4523

Journal of Law and Politics (JLP), 2026; 7(2), 69-83.

jlp.ibupress.com

Online ISSN: 2671-3438

Application: 16.08.2026

Revision: 20.09.2026

Acceptance: 21.10.2026

Publication: 25.10.2026

Rayhan, A. (2026). Artificial intelligence & the violation of right to privacy under article 17 of the ICCPR. Journal of Law and Politics, 7(2), 69-83. https://doi.org//10.69648/CUYL4523

Md. Arif Rayhan

Supreme Court of Bangladesh, Dhaka, Bangladesh

https://orcid.org/0009-0003-9672-1039

Correspondence concerning this article should be addressed to Md. Arif Rayhan, Email: rayhanarif1997@gmail.com

Abstract

Artificial Intelligence (AI) has driven innovation and also has posed greater threats to the privacy rights guaranteed by Article 17 of the International Covenant on Civil and Political Rights (ICCPR). AI systems allow for surveillance, profiling, data fusion and automated decision-making; many of them offer little transparency, consent or accountability. This study employs a doctrinal legal methodology to analyse Article 17's interpretive jurisprudence, while drawing comparative insights from frameworks like the GDPR. It examines how AI practices often involve unlawful inferences when lacking a clear legal basis and arbitrary interference that does not meet the requirements of proportionality, necessity and reasonable standards. Case studies show violations by facial recognition at protests, algorithmic profiling of behaviours and discrimination over health topics, highlighting intersections with the non-discrimination guarantees in Article 26. Findings illustrate that remedies are still insufficient, and States struggle to ensure oversight, effective redress and privacy-by-design protections. The paper ends by arguing that Article 17 must be broadly interpreted to cover informational, algorithmic and biometric privacy, which demands more sophisticated governance and independent regulation and protection of enforceable rights of access, correction and erasure to protect human dignity in the age of AI.

Keywords: Digital privacy, artificial intelligence (AI), GDPR, informational privacy, AI governance.

BALKAN JOURNALS

Introduction

AI plays a crucial role in protecting privacy as it becomes increasingly omnipresent in how society manages sensitive data. Algorithms specifically designed with privacy as a fundamental principle, such as differential privacy, homomorphic encryption, and federated learning, are essential for safeguarding personal information (Rahulamathavan et al., 2024). Developing privacy-focused AI systems requires collaboration among technologists, ethicists, policymakers, and the broader community to establish standards and ensure compliance with legislation. Algorithms and techniques for securing data privacy in AI healthcare solutions (Jeelani et al., 2024). Also, global efforts are essential to regulate AI systems ethically while safeguarding individual privacy.

The development of AI raises serious concerns about the protection and privacy of individuals' personal data, particularly when states or other actors use personal data, directly or indirectly, for surveillance or mass data analysis. The European Union has implemented comprehensive regulations such as the General Data Protection Regulation (GDPR) to address these issues (Hoofnagle et al., 2019), but some provisions could hinder the progress of AI algorithms and machine learning and thus stifle innovation. This article will examine whether the development of AI can fully accommodate the obligations imposed by the GDPR without paralysing artistic and technical creativity, while focusing on the ways in which the human right relating to privacy protected under Article 17 of the ICCPR is being violated by the unregulated use of AI.

Legal Framework: Article 17 of the ICCPR And the Right to Privacy

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) is a cornerstone of privacy rights, dignity, and autonomy for humans, and modern AI systems pose a significant challenge to its guarantees. Article 17 prohibits arbitrary or illegal interference with a person's privacy, family, home, or correspondence. Fast-paced and widespread deployment of AI systems constitutes a rapid, systematic, and often unchallenged violation of this fundamental right of privacy, where AI facilitates an interference that is both illegal, due to a lack of legal frameworks and significant consent, and arbitrary, due to its disproportionate nature, impervious, and suspicious nature (Al-Dulaimi & Mohammed, 2026).

Privacy safeguards must apply to both personal data in fixed technologies and data captured during seamless, mobile interactions or from multiple data sources. Privacy involves the freedom to hold philosophical views without interference, as well as the right to look for, acquire, and transmit information and ideas through whatever means are available (ALibeigi et al., 2019). States have obligations to respect, guarantee, protect, and fulfil the right to privacy. Respect requires refraining from interference; obliges States to prevent interference by third parties; protection obliges States to take measures to safeguard privacy (Rona & Aarons, 2016); and also obliges States to take positive action and provide effective remedies. Interference occurs when the data collected can identify, locate, or profile an individual (Benoist, 2008). The permissible limitations include legal bases for interference, a legitimate aim, and a proportionality test, providing satisfactory evidence to justify each level. Relevant considerations include the exclusion of arbitrary or abusive features of surveillance; the balancing of the degree of interference against the aim; its appropriateness in light of democratic societies or the status of developing countries (Franks, 2017; Mohan, 2025); and the availability of effective remedies and redress. Privacy thus encompasses protection against the indiscriminate or unjustified collection of reliable data. The right to access, rectify, erase, and block personal data is directly relevant, provided it is not incompatible with the right to privacy (ALibeigi et al., 2019).

Any intrusion into a person's private life is unlawful only if the interference is not prescribed by law, and such law must be publicly accessible, precise, and predictable in its application. On the other hand, an interference that is not reasonable, proportionate, or necessary in the circumstances, even if it is technically 'lawful'. It must be based on justifiable grounds and include procedural safeguards. AI systems interfere with privacy in ways that are often unlawful (lacking a proper legal basis) and frequently arbitrary (disproportionate and lacking safeguards) (Gilani et al., 2023). This technological transformation goes further beyond the simple collection of data towards a paradigm of interference which is constant and automated. Interference is not just a potential future risk but a current reality (Osoba & Welser, 2017), which manifests itself in a frequently illegal way, lacking a clear and accessible legal basis and also deeply arbitrary, as it 'frequently does not pass the tests of necessity, proportionality and reasonableness' (Karliuk, 2023).

The Legal Standard: Deconstructing Article 17 of the ICCPR

To evaluate the impact of AI, first we must analyse the thresholds of legal specifics established by Article 17. The provision prohibits two different types of interference:

- **Unlawful Interference:** Any interference that is not prescribed by domestic law. This law must itself be accessible, accurate and predictable in its application (Anghel, 2023), providing the citizens with adequate and appropriate notice of the circumstances in which the authorities may intrude on their privacy.
- **Arbitrary Interference:** This goes further beyond the mere illegality. Even an interference which is technically "legal" should not be arbitrary. According to the United Nations Human Rights Committee, any interference must have procedural protections against abuse and be fair and proportional to a legitimate goal Office of the United Nations High Commissioner for Human Rights, 2018).

Any assessment of the impact of AI on privacy must, therefore, ask two questions: Does an appropriate law exist that authorises this interference? And is the interference, in its scope and application, reasonable and proportionate?

Conceptualisation of the Algorithmic Intruder

Data science is a global phenomenon in which individuals, states, and private actors actively participate to serve their own interests, which are nevertheless ultimately collective (Stephenson, 2015; Turrell, 2025). The terms "data processing", "profiling", and "inference" are therefore broadly defined. Conventional definitions of data collection, processing, and/or profiling each have their limitations; for example, there are various ways to extract knowledge from audio or text files. Processing encompasses all forms of organising, structuring, storing, preserving, acquiring, cataloguing, disseminating, combining, transforming, and any other way of making data accessible (Jambwa, 2003). It therefore includes all means by which data, from various sources and formats, are integrated into a digital system and/or remain there for further combination and exploration. Profiling and inference fall under an analytical dimension (Reeve, 2013), the distinction lying in the obviousness, permanence, or reversibility of the process or information sought. Included are all forms of exploration, analysis, manipulation and/or interpretation of data already selected, stored, retained or otherwise accessible via algorithms and code.

V. Data Collection, Processing and Profiling in AI Systems

All types of algorithmic systems require some information, commonly referred to as data. Data can typically be classified into five main categories: text, images, audio, video, and combinations of multiple data types (Grewal et al., 2021). The feasibility of data collection and user consent largely depends on the respective data processing laws governing the relevant field (Mazhar, 2021). For example, the professional conduct of the recording industry, student information databases, health records, and user behaviour analysis techniques all inherently describe and require certain types of transmissible data and specific content. The viability of acquiring aggregated information also depends on the repository and compatibility required for storage, exchange, and collaboration (Block, 2025). Any AI or non-AI system that collects, uses, or learns from one or more types of data typically requires applicable legislation. Should additional classifications or a macro-level combination be introduced, extensive regulations will apply according to the established operating methods and timeline for when the law is invoked, subsequently affecting initially permitted network or contractual arrangements. Security isolations and approaches that conventionally block selective modelling pathways also incentivise, enable, or restrict discretion, respectively (Kotulski et al., 2020).

The use of algorithmic systems to retrieve and integrate accepted sources places them under direct scrutiny and also requires prolific, specific operational knowledge (Yeung, 2018). Conversely, classification as INTRUSION accumulates the substance of collecting target deliverables; action as EXTRACTION scans for efficiency; modelling as CLASSIFICATION operates on status/features; and the implicit action of CUSTOMISING and MAINTAINING enhances an additional incentive (Belkacem et al., 2024). Information phobia charges a legitimate basis for determining legitimacy, opportunity, feasibility, etc. Preserving a thorough and transparent vision persists while awaiting interest in use and overall presentation. Openly processing systems, including 'NEURAL systems, follow an adaptive composition of PREVIOUS and CURRENT and exploit both coreference and the explicit tactic of reversible passive modeling acts demonstrating' (Lindemann, 2025). The output is indeed capable of directly targeting the desired 'INTRUSION RISK' Office of the Comptroller of the Currency [OCC], 2000) category and the 'RESILIENCE RISK' (Hodge & Gemmill, 2025) quality. Situations addressed with such an operational strategy remain open but well-founded.

Intrusion Into Privacy: Mechanisms And Case Studies

Personal privacy is compromised by a range of AI approaches, including surveillance (social media analytics, facial recognition), data fusion (combining facial and gait data from non-cooperative sources), behavioral targeting (online advertising), and algorithmic decision-making (hiring selection, access to credit, medical diagnoses). Four cases illustrate how privacy rights can be undermined when AI is used:

- **Surveillance.** An individual participating in a public demonstration is identified by a publicly accessible facial recognition system, geolocated, and targeted for unauthorised police identification (Gabrielli, 2025). Information about the event and the individual's emotions is aggregated on social media and combined with previously held facial/gait information. These records are retained for an extended period despite a low likelihood of re-contact, contravening Article 17(1) of the International Covenant on Civil and Political Rights (United Nations General Assembly, 1966).
- **Data fusion.** An individual's face is collected in a context that should have been free of gait data but which was correlated by the aggregation of common location traces. Detecting presence at the same social gathering allows the construction of a social graph (Xiao et al., 2024), thus facilitating inferences about lifestyle, preferences, and social networks, with additional scope enabled by crowdfunding from supplementary sources. Aggregated accessibility of such data can provide insights into preferences and habits (McNicoll, 2002).
- **Behavioral targeting.** A mother's health concerns in a messaging group are exploited to trigger unsolicited and inappropriate advertisements targeting family planning instruments via a video service platform.
- **Algorithmic decision-making.** Desires and preferences regarding intimate relationships are extracted from usage patterns on an adult content platform; this "intimate graph" (Hu & Ge, 2026) of preferences is compared to open data available from job search agencies to exclude certain profiles from job opportunities due to anticipated discrepancies with these desires.

Numerous academic studies and policy documents confirm that such activities conflict with the principles of proportionality, necessity, and legitimate aim (Anđelković, 2017); however, remedies for rights violations associated with these scenarios remain unclear.

Equality, Non-Discrimination and Privacy in AI Governance

The relationship between privacy and a range of criteria that 'inform equality and non-discrimination underpins the obligations arising from Article 26 of the ICCPR' (Australian Government Attorney-General's Department Home, 2025) and other international human rights standards. The monitoring of the right to privacy by AI systems can lead to violations that infringe upon the protections of Article 26. These systems can interfere with the provisions of Article 26 by collecting data targeting ethnic and national origin, race, sex, language, religion, and disability, as well as by engaging in profiling.

The harm to privacy caused by such intervention might include discrimination, prejudice, and unfair treatment of groups such as women, people with disabilities, and members of minorities. In light of the Sustainable Development Goals, the 2030 Agenda for Sustainable Development, and the Convention on the Rights of Persons with Disabilities, which stress the necessity of removing gender bias from AI systems and the significance of upholding the dignity of people with disabilities and preventing discrimination against them, addressing these harms is especially important. The intersection of privacy and equality, non-discrimination, and related rights is therefore a central concern in the design and implementation of sufficiently protective AI governance frameworks (Joseph & Anantharaman, 2024). Respect for the right to privacy thus coexists with and supports parallel obligations regarding equality and non-discrimination.

State Obligations and Extraterritorial Dimensions

At the national level, states are frequently required to enact, regulate, oversee, and enforce sufficient safeguards for privacy and associated rights. Under the ICCPR, states also remain responsible for the effects on these rights of their actions that have extraterritorial or cross-border aspects (Wenzel, 2008). States may need to fulfil obligations of international cooperation when private actors under their jurisdiction operate algorithmic systems that, without a legal basis, infringe on the privacy of individuals located outside their national jurisdiction (Office of the United Nations High Commissioner for Human Rights, 2018). Governments that conclude international treaties or arrangements also commit to respecting them in the relevant external jurisdictions. Trade agreements and other arrangements involving cross-border data flows also have implications for the scope of control over data processing and for the capacity to regulate algorithmic systems.

Recourse, Accountability and Reparation for Privacy Violations

AI systems' widespread data collecting, processing, inference, and profiling run the potential of infringing on the privacy rights guaranteed by Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Many unilateral actions, often carried out by private entities on behalf of states, constitute sufficient interference to trigger ICCPR protections. Such actions can lead to exposure, discrimination, and stigmatisation, posing disproportionate risks to vulnerable groups. Yet, available and feasible remedies remain limited, and significant barriers hinder accountability and redress.

States are obligated to implement effective legislative, regulatory, and policy measures to ensure protection against undue and unjustified invasions of data privacy. When these protections are inadequate or ineffective, individuals are left without access to effective remedies, whether at the national level or through civil society actors. Even when regulations appear robust in theory, a lack of effective implementation means that remedies are often unavailable in practice.

Following the deployment of AI, the burden of proof regarding attribution and harm often falls on affected individuals (Teo, 2025), and many are unaware of their right to redress. Furthermore, disproportionate protection processes are concentrated in the public sector (Maor, 2020), where regulatory activity is most significant, leaving private parties largely outside the scope of enforcement. Where standards exist, they are poorly calibrated to the specificities of algorithmic data processing and surveillance, and 'institutional mechanisms tend to be based on retrospective access monitoring rather than continuous control adapted to the algorithm's full lifecycle' (Janssen & Kuk, 2016). Such approaches offer no significant protection against control exercises carried out by the data controller on behalf of a public party and tend to focus on providing information as the primary accountability mechanism, rather than on the relevance and effectiveness of the measures considered or adopted.

Comparative Perspectives: International Standards and Best Practices

As previously explained, States are required under Article 17 of the ICCPR to respect, safeguard, and uphold the right to privacy. It is crucial to remember that these duties do not prohibit private actors from interfering; in fact, private actors'

involvement is covered by Article 17 as the State usually takes on a role of monitoring, enabling, and/or enforcing in such circumstances.

Article 17 prohibits any arbitrary or unlawful interference, regardless of the means or technologies employed. Algorithms challenge existing privacy protections, but they fall within the definition of privacy articulated by the treaty bodies like the Human Rights Committee (HRC), the Committee on the Rights of the Child (CRC Committee), etc. A clear understanding of the specific challenges imposed allows for an assessment of the compatibility of existing measures with international standards (Delgado Rodrigues & Grossi, 2007) and consequently, the identification of priority areas for reform. Comparisons with European and national frameworks reveal encouraging practices regarding transparency, broader definitions of data processing, additional safeguards concerning profiling, and the recognition of the right to privacy as a fundamental safeguard against algorithmic decision-making.

The increasing use of data-driven AI systems capable of profiling and making high-stakes decisions underscores the need to safeguard the right to privacy (Nkomalago, 2024). Such AI systems operate across a multitude of platforms, justifying the immediate establishment of governance mechanisms inspired by established privacy frameworks. Initial recommendations include conducting risk assessments and implementing regulatory and accountability architectures that prioritise privacy protection (Humerick, 2018).

Policy Implications and Recommendations

The rapid pace of technological innovation in AI and its increasing interconnectedness across industries are challenging global efforts to protect data and privacy. At the same time, privacy and data protection have become critical regulatory issues for businesses and governments. New legislative and regulatory frameworks are evolving to safeguard sensitive personal information, but growing concerns are also emerging about their potential negative impact on AI innovation and use, particularly the General Data Protection Regulation (GDPR) in the European Union (EU) and the California Consumer Privacy Act (CCPA).

AI technology governance requires addressing the conflicts and alignment between the risk assessment framework adopted from the 'Privacy-by-Design (PbD) approach' (Mishova, 2025) and the challenge posed by AI algorithms. Once focused on algorithmic transparency and disproportionate risk assessment, regulation has shifted towards a broader public approach that prioritises social acceptance,

human-centred innovation, and wider definitions of risk, despite the dramatic shift in timescale from minutes to nanoseconds. Decisions to invest in algorithmic controls are fundamentally driven not only by corporate ethical codes but also by the need for competitive advantage, trust, and collaboration (Atmaja, 2025); therefore, compliance alone does not guarantee the security of individual data.

Future Challenges: Technological Convergence and Evolving Privacy Standards

Governments must remain vigilant in the face of technological convergence. Four emerging areas could significantly alter thinking about privacy. Biometric modalities (e.g., fingerprints, facial images), edge computing (distributed computing acquisition processors and storage devices), federated learning (decentralized AI federation network inversion across data spaces), and quantum technology (new forms of cryptography) will soon transform AI privacy safeguards. "The pace of convergence is accelerating. Entire technologies, spaces, and infrastructures can be created and consumed in a matter of days in this increasingly globalised digital economy" (Hughes, 2025). In these circumstances, privacy itself is likely to evolve, which has always been the case where rights emerge, frame, and define affiliations. Consequently, existing data does not need to circulate for georeferencing, studying the receptiveness of AI probes, or controlling AI survey sets (Warch et al., 2024). Circumvention industries have emerged around sources of consumer consent. Auditing can abstract from agreed-upon rights or conscientious affliction. Polling effectively provides objective counterfactuals amidst professional contracts where polling almost always involves innovation, enabling higher-quality chaos. The transition to metaverse applications, where real and virtual everyday lives coalesce, suggests that the physical and digital spheres are converging under a single banner (Humerick, 2018).

Conclusion

AI developments have accelerated rapidly worldwide, with countries and regions contending for scientific and economic leadership. However, there are still serious issues with nations' capacity to support the advancement of AI technology while protecting civil and human rights, especially the right to privacy. In 2016, the European Commission proposed the General Data Protection Regulation (GDPR) to ensure comprehensive and effective data protection. However, fundamental

conflicts between the GDPR and the effective development of AI cast serious doubt on the EU's ability to strike an acceptable balance between privacy protection and the freedom necessary for AI growth. A similar disconnect exists in the global discussion on the protection of personal data in AI systems, where certain fundamental rights considerations remain either under-analysed or insufficiently articulated.

At the international level, the International Covenant on Civil and Political Rights (ICCPR) provides the most appropriate framework for analysing privacy protection in the context of AI. Article 17 of the ICCPR articulates the right to privacy, describes the permissible limitations on this right, and establishes the obligations of States to respect and ensure its protection. Applying the privacy protections of Article 17 to AI systems, as they are currently understood and deployed, reveals a substantial and pervasive gap in protection. The concept of the algorithmic intruder, defined in detail, serves as a useful heuristic for identifying and analysing the multiple complex ways in which AI technologies can interfere directly and indirectly with the right to privacy. Examining these modes of interference shows that AI systems, as currently developed and deployed, pose significant privacy risks that remain largely unresolved. The analysis demonstrates States' need to adopt quick and effective measures to fill these gaps and limit the scope of interference with the right to privacy caused by these emergent and fast-growing technologies. Yet one question remains unsolved: if algorithms themselves are becoming the new arbiters of privacy, who or what will ultimately arbitrate the algorithms? And the answer would be dynamic, where a comprehensive approach is needed with a multi-layered governance ecosystem comprising courts, regulators, technical bodies, civil society, and legal instruments.

References

Al-Dulaimi, A. O. M., & Mohammed, M. A. A. W. (2026). Legal responsibility for errors caused by artificial intelligence (AI) in the public sector. *International Journal of Law and Management*, *68*(4), 695–722. https://doi.org/10.1108/IJLMA-08-2024-0295

Alibeigi, A., Munir, A. B., & Karim, M. E. (2019). Right to privacy, a complicated concept to review. *Library Philosophy and Practice*, Article 2841. https://scholarworks.sjsu.edu/libphilprac/2841/

Anđelković, L. (2017). The elements of proportionality as a principle of human rights limitations. *Facta Universitatis, Series: Law and Politics, 15*(3), 235–244. https://doi.org/10.22190/FULP1703235A

Anghel, E. (2023). Predictability and accessibility of the law. *Lex ET Scientia International Journal, 30*(1), 69–78.

Atmaja, S. A. (2025). Ethical considerations in algorithmic decision-making: Towards fair and transparent AI systems. *Riwayat: Educational Journal of History and Humanities, 8*(1), 620–627. https://doi.org/10.24815/jr.v8i1.44112

Australian Government Attorney-General's Department. (2025). *Rights of equality and non-discrimination*. https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/rights-equality-and-non-discrimination

Belkacem, T., Ioualalen, A., Ribeiro, S., Rodriguez, N., Rouffet, J.-B., Bascans, J., & Signe, Q. (2024). *MLEAP: Machine learning application approval: Final report – Executive summary*. European Union Aviation Safety Agency. https://www.easa.europa.eu/sites/default/files/dfu/mleap-d4-public-report-executive_summary_expanded-issue01.pdf

Benoist, E. (2008). Collecting data for the profiling of web users. In M. Hildebrandt & S. Gutwirth (Eds.), Profiling the European citizen: Cross-disciplinary perspectives (pp. 169–184). Springer. https://doi.org/10.1007/978-1-4020-6914-7_9

Block, S. (2025, February 6). *Domain-driven design (DDD): Software architecture best practices*. Rock the Prototype. https://rock-the-prototype.com/en/software-architecture/domain-driven-design-ddd/

Delgado Rodrigues, J., & Grossi, A. (2007). Indicators and ratings for the compatibility assessment of conservation actions. *Journal of Cultural Heritage*, *8*(1), 32–43. https://doi.org/10.1016/j.culher.2006.04.007

Franks, M. A. (2017). Democratic surveillance. Harvard Journal of Law & Technology, 30(2), 425–489. https://doi.org/10.7916/ljlt.v30i2.5043

Gabrielli, G. (2025). The use of facial recognition technologies in the context of peaceful protest: The risk of mass surveillance practices and the implications for the protection of human rights. *European Journal of Risk Regulation, 16*(2), 514–541. https://doi.org/10.1017/err.2025.26

Gilani, S. R. S., Al-Matrooshi, A. M., & Khan, M. H. (2023). Right of privacy and the growing scope of artificial intelligence. *Current Trends in Law and Society, 3*(1), 1–11. https://doi.org/10.52131/ctls.2023.0301.0011

Grewal, R., Gupta, S., & Hamilton, R. (2021). Marketing insights from multimedia data: Text, image, audio, and video. *Journal of Marketing Research, 58*(6), 1025–1033. https://doi.org/10.1177/00222437211054601

Hodge, H., & Gemmill, L. (2025, February 11). *Risk and resilience: Bringing risk management and resilience closer together*. Deloitte. https://www.deloitte.com/uk/en/services/consulting-risk/blogs/2025/risk-and-resilience-bringing-risk-management-and-resilience-closer-together.html

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hu, T., & Ge, L. (2026). Datafication of digital intimacy: The dual logic of empowerment and commodification. *Games and Culture, 21*(7), 1698–1722. https://doi.org/10.1177/15554120251358522

Hughes, H. (2025). *The great convergence: How technology diffusion is accelerating poverty reduction in emerging economies (2000–2050)*. SSRN. https://doi.org/10.2139/ssrn.5739390

Humerick, M. (2018). The tortoise and the hare of international data privacy law: Can the United States catch up to rising global standards? *Catholic University Journal of Law and Technology, 27*(1), 77–126. https://scholarship.law.edu/jlt/vol27/iss1/5

Jambwa, M. M. (2003, November 3). Data processing, analysis, and dissemination (ESA/STAT/AC.93/8) [Conference paper]. United Nations Statistics Division. https://unstats.un.org/unsd/demographic/meetings/egm/sampling_1203/docs/no_8.pdf

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly*, *33*(3), 371–377. https://doi.org/10.1016/j.giq.2016.08.011

Jeelani, O. F., Njie, M., & Korzhuk, V. M. (2024). *Algorithms and techniques for securing data privacy in AI healthcare solutions*. www.tijer.org

Joseph, S., & Anantharaman, V. (2024). Algorithmic bias and human rights: Exploring the intersection and implications. *International Journal of Law Management & Humanities,* 7(1), 1526–1541. https://ijlmh.com/wp-content/uploads/Algorithmic-Bias-and-Human-Rights.pdf

Karliuk, M. (2023). Proportionality principle for the ethics of artificial intelligence. *AI and Ethics*, *3*(3), 985–990. https://doi.org/10.1007/s43681-022-00220-1

Kotulski, Z., Nowak, T. W., Sepczuk, M., & Tunia, M. A. (2020). 5G networks: Types of isolation and their parameters in RAN and CN slices. *Computer Networks, 171,* Article 107135. https://doi.org/10.1016/j.comnet.2020.107135

Lindemann, M. M. (2025). Enhancing structural inductive biases of sequence-to-sequence models for semantic parsing and beyond [Doctoral dissertation, University of Edinburgh]. Edinburgh Research Archive. https://doi.org/10.7488/era/6221

Maor, M. (2020). A disproportionate policy perspective on the politics of crisis management. *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.1513

Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health, 10*(1), 6–10. https://doi.org/10.24321/2319.9113.202101

McNicoll, G. (2002). International encyclopedia of the social & behavioral sciences, 26 vols. *Population and Development Review*, *28*(1), 162–163.

Mishova, A. (2025, April 11). *Privacy by design: Meaning and its importance*. GDPR Local. https://gdprlocal.com/privacy-by-design-meaning/

Mohan, C. (2025). Surveillance and national security: Balancing privacy and public interest for a safer society. In T. Teena, P. Avasthi, S. Yadav, & A. Dixit (Eds.), Proceedings of the National Seminar on Enhancing Privacy Protection in the Digital Age: Legal Challenges & Innovations (pp. 537–561). Atlantis Press. https://doi.org/10.2991/978-2-38476-426-6_26

Nkomalago, M. (2024, March 5). *Privacy-preserving AI algorithms: A necessity for responsible innovation*. LinkedIn. https://www.linkedin.com/pulse/privacy-preserving-ai-algorithms-necessity-innovation-nkomalago-vnwre/

Office of the Comptroller of the Currency. (2000, May 15). Infrastructure threats—Intrusion risks: Message to bankers and examiners (OCC Bulletin 2000-14). https://www.occ.gov/news-issuances/bulletins/2000/bulletin-2000-14.html

Office of the United Nations High Commissioner for Human Rights. (2018, August 3). *OHCHR and privacy in the digital age*. https://www.ohchr.org/en/privacy-in-the-digital-age

Osoba, O. A., & Welser, W., IV. (2017). *The risks of artificial intelligence to security and the future of work* (PE-237-RC). RAND Corporation. https://doi.org/10.7249/PE237

Rahulamathavan, Y., Herath, C., Liu, X., Lambotharan, S., & Maple, C. (2024). *FheFL: Fully Homomorphic Encryption Friendly Privacy-Preserving Federated Learning with Byzantine Users*. http://arxiv.org/abs/2306.05112

Reeve, A. (2013). *Managing data in motion: Data integration best practice techniques and technologies*. Morgan Kaufmann. https://doi.org/10.1016/C2011-0-07758-X

Rona, G., & Aarons, L. (2016). State responsibility to respect, protect and fulfill human rights obligations in cyberspace. *Journal of National Security Law & Policy, 8*(3), 503–530. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2859615

Stephenson, D. (2015, October 7). Data science and EU privacy regulations: A storm on the horizon – Part 1. LinkedIn. https://www.linkedin.com/pulse/data-science-eu-privacy-regulations-storm-horizon-1-david/

Teo, S. A. (2025). Artificial intelligence and its 'slow violence' to human rights. *AI and Ethics*, *5*(3), 2265–2280. https://doi.org/10.1007/s43681-024-00547-x

Turrell, A. (2025). Cutting through complexity: How data science can help policymakers understand the world. In *The economy as an evolving complex system IV* (pp. 342–370). SFI Press. https://doi.org/10.37911/9781947864665.11

United Nations General Assembly. (1966, December 16). *International Covenant on Civil and Political Rights* (General Assembly Resolution 2200A (XXI)). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Warch, D., Stellbauer, P., & Neis, P. (2024). Advanced techniques for geospatial referencing in online media repositories. *Future Internet, 16*(3), Article 87. https://doi.org/10.3390/fi16030087

Wenzel, N. (2008). Human rights, treaties, extraterritorial application and effects. *Max Planck Encyclopedia of Public International Law*. Oxford University Press. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e819

Xiao, Z., Zhao, N., Li, N., Li, C., Wang, K., Shen, Q., & Zhou, Y. (2024). *A social network detection method based on graph network embedding* [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-3829805/v1

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. https://doi.org/10.1111/rego.12158