

Privacy Rights in the Digital Era: Legal Challenges and Regulatory Frameworks

Afzal Ahamad

Research Scholar, Dept of Political Science and Human Rights

Jamia Hamdard, New Delhi-110062

Email: afzal.ahmad2806@gmail.com

Prof. Syed Mehartaj Begum

Head, Dept of Political Science and Human Rights & Dean, School of Humanities and Social Sciences

Jamia Hamdard, New Delhi-110062

Email: smtaj@jamiahamdard.ac.in

Abstract

The recent exponential growth of digital technologies such as artificial intelligence (AI), big data analytics, social media platforms, and ubiquitous surveillance infrastructures has fundamentally changed the way in which personal information is collected, processed, stored, and shared. In this context, privacy has become a fundamental human right whose protection becomes more and more difficult to guarantee in today's information ecosystems. This paper discusses the right to privacy in the digital age by reviewing the major legal challenges and the evolution of regulatory frameworks at the international, regional and domestic levels. Building on socio-legal studies of AI and human rights, as well as scholarship on data protection and corporate responsibility, the paper highlights how algorithmic bias, mass surveillance, opaque decision-making systems, and cross-border data flows undermine traditional understandings of privacy and informational self-determination. It then goes on to discuss major regulatory responses such as the right to privacy in international human rights law, the European Union's General Data Protection Regulation (GDPR) and emerging data protection measures in India and considers whether these are sufficient to address present-day risks.

The paper argues that, for effective protection of privacy in the digital era, strong legal norms alone are not sufficient, and that ethics-by-design, algorithmic transparency and context-specific governance mechanisms that include human rights impact assessment and meaningful accountability for states and private actors are also needed.

Keywords: Privacy rights; digital era; artificial intelligence; data protection; GDPR; India.

Introduction

Privacy is often regarded as an essential right for human dignity, autonomy and democratic participation. Many international instruments protect the right to privacy. One of the articles is article 17 of ICCPR that prohibits any unlawful and arbitrary interference with the privacy, family, home or correspondence of any individual*. But in the digital age privacy is more vulnerable because of the exponential increase in the amount, speed and specificity of personal data collection. The modern data ecosystem and AI-powered analytics allow new modes of profiling, behavior prediction and micro-targeting that challenge existing legal classifications and enforcement procedures†.

* Chatterjee, S., & Sreenivasulu, N. S. (2021). Artificial intelligence and human rights: A comprehensive study from Indian legal and policy perspective. *International Journal of Law and Management*. <https://doi.org/10.1108/IJLMA-02-2021-0049>

† Shin, D. D., Fotiadis, A., & Yu, H. (2019). Prospectus and limitations of algorithmic governance: An ecological evaluation of algorithmic trends. *Digital Policy, Regulation and Governance*, 21(4), 369–383. <https://doi.org/10.1108/DPRG-03-2019-0017>

And the rise of artificial intelligence and machine learning is pouring fuel on the fire, creating new questions around data protection and privacy. Artificial intelligence systems require lots of data and that data can include personally identifiable information. The output of AI systems is based on statistical patterns and can reflect and reinforce social biases. Such systems are used in prisons, health insurance, employment and credit ratings. They infringe upon people's rights to privacy and equality by invasive inference and constant surveillance[‡]. Some researchers have therefore argued for privacy rights to be included in the wider human rights issues arising from algorithmic government and AI[§]. In data-rich countries such as India, the problem of privacy is complicated by the fact that regulations are not always applied evenly and digitization is happening fast. Laws do a poor job of protecting the ubiquitous connectivity and data-driven services that digital platforms and telecom companies offer^{**}. Some personal data is protected under the Information Technology Act, 2000 and the rules made there under. However, lack of robust data protection laws makes people vulnerable to invasive data practices and poor accountability^{††}. The debates on the draft data protection bill of the Srikrishna Committee and the contours of an Indian data protection regime are reflective of the larger global struggles to reconfigure privacy law to the realities of AI-enabled surveillance and platform capitalism^{‡‡}.

This paper will attempt to contribute to these debates through a socio-legal analysis of digital privacy rights with special emphasis on the regulatory frameworks and legal challenges. First, it examines the philosophical basis of privacy and informational self-determination. Secondly, the main legal challenges raised by digital technologies and thirdly, the evolution and limits of regulatory solutions at international, European and Indian levels. always stressing the need for ethics-by-design, human rights due diligence and multi-stakeholder governance to protect privacy in today's information societies^{§§}.

Privacy in the Age of Datafication: Power, Consent, and Surveillance

There are many different ways to think about privacy over time. These include concepts of the home as private space, control over personal information and decisional autonomy in intimate matters^{***}. With the advent of the digital age, concerns about privacy of information have grown ever more pressing as people have interacted with complex socio-technical systems that continuously produce, collect and analyses data on their behavior, preferences and relationships. Other scholars have argued that privacy is not a right to secrecy or individual control, but rather a relational and contextual right shaped by social norms, power relations and institutional practices.

Privacy in AI-based contexts is closely related to the right of informational self-determination, i.e. the right of individuals to decide about the collection, use and dissemination of personal data. But traditional consent-based regimes have been shown to be inadequate in the face of opaque algorithms, complex data flows and knowledge asymmetries between data subjects and data controllers. Often consent is not meaningful and

[‡] Lauren, G. (2021). Facial recognition software is biased towards white men, researcher finds. The Verge. <https://www.theverge.com>

[§] Miao, Z. (2019). Investigation on human rights ethics in artificial intelligence researches with library literature analysis method. The Electronic Library, 37(5), 914–926. <https://doi.org/10.1108/EL-04-2019-0089>

^{**} Sahay, A., & Tiwari, T. (2018). Airtel pricing in the cannibalisation era and transition to data. Indian Institute of Management Ahmedabad case study. <https://doi.org/10.1108/CASE.IIMA.2020.000118>

^{††} Sumanjeet. (2010). The state of e-commerce laws in India: A review of information technology act. International Journal of Law and Management, 52(4), 265–282.

^{‡‡} Chatterjee, S., & Sreenivasulu, N. S. (2019). Personal data sharing and legal issues of human rights in the era of artificial intelligence: Moderating effect of government regulation. International Journal of Electronic Government Research, 15(3), 21–36. <https://doi.org/10.4018/IJEGR.2019070102>

^{§§} Ibricu, B., & van der Made, M. L. (2020). Ethics by design: A code of ethics for the digital age. Records Management Journal, 30(3), 395–414. <https://doi.org/10.1108/RMJ-08-2019-0044>

^{***} Miller, L. F. (2014). Is species integrity a human right? A rights issue emerging from individual liberties with new technologies. Human Rights Review, 15(2), 177–199. <https://doi.org/10.1007/s12142-013-0287-x>

people do not have a meaningful understanding of how their data will be processed or how automated decisions may affect them, exposing them to invasive profiling and surveillance. Such concerns have resulted in demands for more rights of explanation, correction, objection and deletion in data protection law.

And privacy is inextricably linked with the wider socio-economic structures such as platform business models and state security practices. Personal data is a strategic asset for corporate actors, with revenues associated with pervasive tracking and behavioral analytics. States are deploying surveillance technologies enabled by AI in the name of security and efficiency^{†††}. The datafication of society raises concerns of collective privacy, group discrimination and digital inequality as marginalized communities are disproportionately subjected to intrusive monitoring and experimental technologies^{‡‡‡}. A strong privacy framework must be able to counteract the power of the individual as well as the power of the structure, so that data practices do not undermine human rights or reinforce existing hierarchies.

Legal Challenges to Privacy in the Digital Era

The rise of AI and big data analytics in governance and commercial decision-making has generated a host of legal challenges for the protection of privacy rights. There are four interrelated issues to watch: mass surveillance, algorithmic bias and discrimination, cross-border data flows and weak corporate accountability.

1. Technologies such as facial recognition, predictive policing and AI monitoring of online interactions have made it easier for governments and businesses to monitor people in public and private places. In 2021, governmental system monitoring facilities found that police facial recognition systems are likely to misidentify non-white faces as white faces and produce erroneous results. This can lead to wrong arrests and restrictions on people's freedom of movement and association. Also, AI-powered risk scoring tools in criminal justice have come under fire for perpetuating historic biases and eroding the right to a fair trial. This has raised concerns about the extent to which these systems function in relation to human rights law protections of privacy and due process^{§§§}.
2. Second, algorithms are huge privacy issues with bias and discrimination. Bias can be induced by biased training data, weak statistical assumptions, or design choices that embed societal biases into data processing systems. Computers generate labels that can make people and groups feel bad about themselves^{****}. AI systems are opaque, sometimes called "black box models," and people cannot always understand or challenge the conclusions those systems draw. This restricts the opportunities for individuals to engage traditional legal remedies rooted in openness and responsibility^{††††}.
3. Third, privacy rules have difficulty covering large areas due to data colonialism and cross-border data flows. Global platforms and cloud infrastructures raise questions about the applicability of laws and the ability of individuals to assert rights in relation to data created in one jurisdiction and processed in another. When personal data is

^{†††} Bernaz, N. (2013). Enhancing corporate accountability for human rights violations: Is extraterritoriality the magic potion? *Journal of Business Ethics*, 117(3), 497–511. <https://doi.org/10.1007/s10551-012-1531-z>

^{‡‡‡} Bogoviz, A. V. (2020). Perspective directions of state regulation of competition between human and artificial intellectual capital in industry 4.0. *Journal of Intellectual Capital*, 21(4), 583–600. <https://doi.org/10.1108/JIC-11-2019-0270>

^{§§§} Nikolaos, A., Dimitrios, T., Daniel, P., & Vasileios, L. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, 2, e93. <https://doi.org/10.7717/peerj-cs.93>

^{****} Krkac, K. (2019). Corporate social irresponsibility: Humans vs artificial intelligence. *Social Responsibility Journal*, 15(6), 786–802. <https://doi.org/10.1108/SRJ-09-2018-0219>

^{††††} Losbichler, H., & Lehner, O. M. (2021). Limits of artificial intelligence in controlling and the ways forward: A call for future accounting research. *Journal of Applied Accounting Research*, 22(2), 365–382. <https://doi.org/10.1108/JAAR-10-2020-0207>

sent to foreign companies that are technology-strong but don't adequately protect human rights, the risk of abuse increases and domestic regulatory efforts are hampered. Debates on data localization and digital sovereignty are examples of people trying to take back control of these flows. At the same time, they raise questions about the increasing fragmentation of the internet and its possible effect on data-driven innovation in the legal field.

4. Fourth, it remains a challenge to hold corporations accountable. Traditionally, human rights frameworks have been focused on states, but recent discussions have started to acknowledge the growing power of private corporations over digital infrastructures and data practices. Without sufficient oversight, developers of artificial intelligence (AI), data brokers, and media and ICT companies can violate privacy and associated rights through surveillance, behavioral targeting, and opaque algorithmic decision-making. Soft law instruments, such as the UN Guiding Principles on Business and Human Rights, highlight the responsibility of corporations to respect human rights. However, their use within the digital realm has been sporadic and there are few binding pledges for privacy and data protection.

Regulatory Frameworks for Privacy Protection

In response to growing threats to privacy, a variety of regulatory regimes have emerged at the international, regional and domestic levels. This section discusses three key regimes namely international human rights law, the EU's General Data Protection Regulation (GDPR) and emerging data protection initiatives in India.

International human rights law sets the minimum standard for privacy protection. The ICCPR Article 17 on arbitrary or unlawful interference with privacy and freedom of expression, association and non-discrimination clauses are part of the larger human rights context of privacy (Chatterjee & Sreenivasulu, 2021; Zhai et al., 2020). Privacy and data protection are similarly recognized as fundamental rights by regional instruments such as the European Convention on Human Rights and the EU Charter of Fundamental Rights. "States must strike a balance between these rights and legitimate objectives such as security and public order with individual freedoms." The European Court of Human Rights has in its recent case law stressed the importance of safeguards against mass surveillance, data retention and indiscriminate collection of metadata. This suggests that AI-enabled monitoring should be tightly constrained by law and subject to independent oversight.

The GDPR is one of the most extensive data protection frameworks in force today. It provides principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and gives data subjects rights to information, access, rectification, erasure, restriction of processing, data portability and objection. "GDPR provisions on data protection impact assessments, accountability mechanisms and safeguards against automated decision-making offer important tools to address risks to privacy arising from AI. But they also point out that the rule is challenged by non-explainable AI systems and complex data ecosystems, where even the creators may not understand the logic behind the algorithm.

The data protection law in India is in transition. The Information Technology Act 2000 and the rules offer limited protection primarily for cybercrime and intermediary liability but not for comprehensive privacy rights^{****}. Recognizing the need for stronger safeguards, the Srikrishna Committee recommended a draft data protection bill in 2018. The bill tackled consent, data minimization and accountability and proposed the establishment of a Data Protection Authority to monitor compliance. The bill has travelled through a long and amended legislative process, but the deliberations have also brought issues such as data

^{****} Sharma, C., & Kaushik, A. (2017). Strategy for privacy assurance in offshoring arrangements. *Journal of Global Operations and Strategic Sourcing*, 10(2), 232–254. <https://doi.org/10.1108/JGOSS-10-2016-0030>

localization, state surveillance and exemptions for national security to the forefront of public discussion. Study have made the case that any future Indian data protection regime must incorporate human rights principles, provide for effective oversight of state and private actors, and deal with structural inequalities that determine the experience of privacy across different social groups.

Detail study analyzed AI ethics guidelines published by governments, industry bodies and international organizations. Most of them revolve around transparency, fairness, accountability and privacy by design but lack enforcement mechanisms often. An ethics by design approach is proposed which embeds ethical principles in organizational processes and technical architectures, explicitly taking into account data protection and privacy at each stage of the AI lifecycle. Such frameworks can help govern law by encouraging organizational cultures that value human rights and by providing practical tools for implementing privacy protections in complex digital systems.

Discussion and Recommendations

The above study shows that the existing legal and regulatory frameworks have major flaws, but at the same time, they offer important tools for the protection of privacy rights in the digital age. International human rights law, and instruments such as the GDPR and the proposed Indian data protection law, give us a lot of general rules and detailed rules on how to treat data. However, they are less useful due to challenges of regulation, ambiguity of technology and unequal power distribution.

1. The first suggestion is to enhance the investigation about how the algorithms work and how they affect human rights. Governments or private companies using AI to process personal data should be required to conduct privacy risk assessments before and after the use of the AI, including assessments of the risk of discriminatory effects, and to share summaries of their findings. Data security authorities and ombud institutions should be independent oversight bodies that can review these assessments, require corrections to be made for errors and, if necessary, penalize violators.
2. Ethics-by-design and privacy-by-design should both include privacy-by-design as an element. Businesses must consider ethics and human rights when designing, building and using AI systems. This should include clear rules on how much data to collect, what it can be used for, and people's right to be told why. Technical steps that can help reduce privacy risks include differential privacy, federated learning, and strong access controls. But this needs to be combined with an organization's willingness to be open and responsible.
3. Regulatory structures need to take into account the structural dimensions of digital inequality. AI and data-driven systems can lead to greater social and economic inequalities by unfairly targeting or excluding disadvantaged groups. So, privacy law should shield people from hurting others, promote collective participation in decision-making and make it simple and effective for the most vulnerable to get help.
4. Finally, countries need to work together very hard to regulate cross border data flows and avoid data colonialism. States should cooperate in multilateral fora to set up jurisdictional rules, agree on common privacy and data protection standards, and incentivize each other to help enforcement to avoid a regulatory race to the bottom that undermines protections in the name of innovation. Working together in this way can help ensure that national laws are consistent with international human rights standards and that everyone's privacy rights are protected online.

Conclusion

Surveillance, algorithmic profiling and complex data ecosystems powered by AI pose challenges to privacy rights never seen before in the digital age. There are important legal and normative regimes such as the GDPR, international human rights law, and new data security initiatives in India. However, they need to be improved and enforced more strictly to address the technological lack of clarity, structural inequality and the flow of data across borders. States and businesses can better protect the right of people to privacy as a basic human right in today's information societies through the application of human rights impact assessment, ethics-by-design, and multi-stakeholder governance to their digital policies and practices.

References

1. Bernaz, N. (2013). Enhancing corporate accountability for human rights violations: Is extraterritoriality the magic potion? *Journal of Business Ethics*, 117(3), 497–511. <https://doi.org/10.1007/s10551-012-1531-z>
2. Bogoviz, A. V. (2020). Perspective directions of state regulation of competition between human and artificial intellectual capital in industry 4.0. *Journal of Intellectual Capital*, 21(4), 583–600. <https://doi.org/10.1108/JIC-11-2019-0270>
3. Chatterjee, S., & Sreenivasulu, N. S. (2019). Personal data sharing and legal issues of human rights in the era of artificial intelligence: Moderating effect of government regulation. *International Journal of Electronic Government Research*, 15(3), 21–36. <https://doi.org/10.4018/IJEGR.2019070102>
4. Chatterjee, S., & Sreenivasulu, N. S. (2021). Artificial intelligence and human rights: A comprehensive study from Indian legal and policy perspective. *International Journal of Law and Management*. <https://doi.org/10.1108/IJLMA-02-2021-0049>
5. Ibiricu, B., & van der Made, M. L. (2020). Ethics by design: A code of ethics for the digital age. *Records Management Journal*, 30(3), 395–414. <https://doi.org/10.1108/RMJ-08-2019-0044>
6. Krkac, K. (2019). Corporate social irresponsibility: Humans vs artificial intelligence. *Social Responsibility Journal*, 15(6), 786–802. <https://doi.org/10.1108/SRJ-09-2018-0219>
7. Lauren, G. (2021). Facial recognition software is biased towards white men, researcher finds. *The Verge*. <https://www.theverge.com>
8. Losbichler, H., & Lehner, O. M. (2021). Limits of artificial intelligence in controlling and the ways forward: A call for future accounting research. *Journal of Applied Accounting Research*, 22(2), 365–382. <https://doi.org/10.1108/JAAR-10-2020-0207>
9. Methven O'Brien, C., & Dhanarajan, S. (2016). The corporate responsibility to respect human rights: A status review. *Accounting, Auditing & Accountability Journal*, 29(4), 542–567. <https://doi.org/10.1108/AAAJ-09-2015-2230>
10. Miao, Z. (2019). Investigation on human rights ethics in artificial intelligence researches with library literature analysis method. *The Electronic Library*, 37(5), 914–926. <https://doi.org/10.1108/EL-04-2019-0089>
11. Miller, L. F. (2014). Is species integrity a human right? A rights issue emerging from individual liberties with new technologies. *Human Rights Review*, 15(2), 177–199. <https://doi.org/10.1007/s12142-013-0287-x>
12. Nikolaos, A., Dimitrios, T., Daniel, P., & Vasileios, L. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, 2, e93. <https://doi.org/10.7717/peerj-cs.93>
13. Ryan, M., & Stahl, B. C. (2021). Artificial intelligence ethics guidelines for developers and users: Clarifying their content and normative implications. *Journal of*

- Information, Communication and Ethics in Society, 19(1), 61–86. <https://doi.org/10.1108/JICES-12-2019-0138>
14. Sahay, A., & Tiwari, T. (2018). Airtel pricing in the cannibalisation era and transition to data. Indian Institute of Management Ahmedabad case study. <https://doi.org/10.1108/CASE.IIMA.2020.000118>
 15. Sarikakis, K., Korbiel, I., & Piassaroli Mantovaneli, W. (2018). Social control and the institutionalization of human rights as an ethical framework for media and ICT corporations. Journal of Information, Communication and Ethics in Society, 16(3), 275–289. <https://doi.org/10.1108/JICES-02-2018-0018>
 16. Sharma, C., & Kaushik, A. (2017). Strategy for privacy assurance in offshoring arrangements. Journal of Global Operations and Strategic Sourcing, 10(2), 232–254. <https://doi.org/10.1108/JGOSS-10-2016-0030>
 17. Shin, D. D., Fotiadis, A., & Yu, H. (2019). Prospectus and limitations of algorithmic governance: An ecological evaluation of algorithmic trends. Digital Policy, Regulation and Governance, 21(4), 369–383. <https://doi.org/10.1108/DPRG-03-2019-0017>
 18. Sumanjeet. (2010). The state of e-commerce laws in India: A review of information technology act. International Journal of Law and Management, 52(4), 265–282.

Bibliography

Journal Articles & Reports

1. N. Bernaz, Enhancing corporate accountability for human rights violations: Is extraterritoriality the magic potion?, 117(3) *Journal of Business Ethics* 497 (2013).
2. A. V. Bogoviz, Perspective directions of state regulation of competition between human and artificial intellectual capital in industry 4.0, 21(4) *Journal of Intellectual Capital* 583 (2020).
3. S. Chatterjee & N. S. Sreenivasulu, Personal data sharing and legal issues of human rights in the era of artificial intelligence: Moderating effect of government regulation, 15(3) *International Journal of Electronic Government Research* 21 (2019).
4. S. Chatterjee & N. S. Sreenivasulu, Artificial intelligence and human rights: A comprehensive study from Indian legal and policy perspective, *International Journal of Law and Management* (2021).
5. B. Ibiricu & M. L. van der Made, Ethics by design: A code of ethics for the digital age, 30(3) *Records Management Journal* 395 (2020).
6. K. Krkac, Corporate social irresponsibility: Humans vs artificial intelligence, 15(6) *Social Responsibility Journal* 786 (2019).
7. H. Losbichler & O. M. Lehner, Limits of artificial intelligence in controlling and the ways forward: A call for future accounting research, 22(2) *Journal of Applied Accounting Research* 365 (2021).
8. C. Methven O'Brien & S. Dhanarajan, The corporate responsibility to respect human rights: A status review, 29(4) *Accounting, Auditing & Accountability Journal* 542 (2016).
9. Z. Miao, Investigation on human rights ethics in artificial intelligence researches with library literature analysis method, 37(5) *The Electronic Library* 914 (2019).
10. L. F. Miller, Is species integrity a human right? A rights issue emerging from individual liberties with new technologies, 15(2) *Human Rights Review* 177 (2014).
11. A. Nikolaos, T. Dimitrios, P. Daniel, & L. Vasileios, Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective, 2 *PeerJ Computer Science* e93 (2016).
12. M. Ryan & B. C. Stahl, Artificial intelligence ethics guidelines for developers and users: Clarifying their content and normative implications, 19(1) *Journal of Information, Communication and Ethics in Society* 61 (2021).
13. A. Sahay & T. Tiwari, Airtel pricing in the cannibalisation era and transition to data, *Indian Institute of Management Ahmedabad Case Study* (2018).
14. K. Sarikakis, I. Korbiel, & W. Piassaroli Mantovaneli, Social control and the institutionalization of human rights as an ethical framework for media and ICT corporations, 16(3) *Journal of Information, Communication and Ethics in Society* 275 (2018).
15. C. Sharma & A. Kaushik, Strategy for privacy assurance in offshoring arrangements, 10(2) *Journal of Global Operations and Strategic Sourcing* 232 (2017).
16. D. D. Shin, A. Fotiadis, & H. Yu, Prospectus and limitations of algorithmic governance: An ecological evaluation of algorithmic trends, 21(4) *Digital Policy, Regulation and Governance* 369 (2019).
17. Sumanjeet, The state of e-commerce laws in India: A review of information technology act, 52(4) *International Journal of Law and Management* 265 (2010).

Web Sources

18. G. Lauren, "Facial recognition software is biased towards white men, researcher finds," *The Verge* (2021), available at <https://www.theverge.com>.