International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Balancing data protection and human rights in the digital age: A review

Srinath Muralinathan *

Computer Science with a focus on Privacy and Security in Data Systems, University of North Carolina at Charlotte.

International Journal of Science and Research Archive, 2025, 16(01), 505-515

Publication history: Received on 26 May 2025; revised on 01 July 2025; accepted on 04 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2031

Abstract

The rapid pace of advancement of digital technology has tremendously influenced the manner of collection, storage, processing, and use of personal data. This situation brought to the fore concerns about data privacy, informational autonomy, and consequences for the fundamental human rights in a digital society. This review seeks to establish the nexus between data protection and essential human rights in contemporary times. It discusses the various international legal regimes and the effectiveness of the GDPR, particularly in the European context, in countering threats of excessive surveillance, unauthorized use of data, algorithmic discrimination, and infringement of personal freedoms. The paper highlights how digital platforms and state surveillance programs impede the exercise of data collection and analysis by corporate entities. A call is made for a rights-based and balanced approach to data governance that supports technological advancement and economic growth while ensuring accountability, transparency, and personal freedoms. The review intends to outline the way forward in order to put into practice measures that achieve the ethical, inclusive, and sustainable data governance paradigms consistent with democratic values, increase public trust, and reflect dignity and rights for individuals in the digital age.

Keywords: Data Protection; Human Rights; Digital Privacy; Surveillance; GDPR; Digital Age; Ethical Data Governance; Algorithmic Bias; Fundamental Freedoms; Cybersecurity

1. Introduction

Modern society has undergone a digital transformation that has led to such an unprecedented increase in data generation and consumption that every pillar that constitutes human life – social, economic, political, and private-is being turned around. It becomes difficult for people to keep their privacy because of internet-connected devices; cloud computing; Artificial Intelligence; and large data analytics, since many governments, large companies, or digital platforms can gain access to personal data and decode individuals [1]. Such a hyper-connectivity would likely engender efficient and innovative ways, but it would also present fundamental human rights—privacy, freedom of expression, and protection from discrimination with significant challenges [3]. The digital age has ushered in new types of laws, such as the GDPR, the CA Consumer Privacy Act, and the Digital Personal Data Protection Act of India, but cross-border data flows and the disparate maturity levels of countries in terms of regulation have made enforcement of these laws difficult. Emerging technologies, such as facial recognition and algorithmic decision-making, worsen these problems and thus require a more balanced form of data governance [4].

1.1. Relevance and Significance of the Topic (Literature Review)

The growing body of academic literature and policy reports investigating the intersections of data protection and human rights demonstrates the foundational conceptual, legal, and technological perspectives upon which works are developed that elaborate on privacy in the digital era. The following Table I summarizes some of the key contributions in this field [5] - [11]

* Corresponding author: Srinath Muralinathan

2. Literature review

Table 1 Key contributions

Author(s)	Year	Title / Study	Key Findings
Solove, D. J.	2006	A Taxonomy of Privacy	Highlights the conceptual ambiguity of privacy and its contextual relevance.
Zuboff, S.	2019	The Age of Surveillance Capitalism	Critiques how corporations exploit personal data for economic gains.
Tufekci, Z.	2015	Algorithmic Harms Beyond Facebook and Google	Explores how opaque algorithms reinforce social inequalities and bias.
Greenleaf, G.	2020	Global Data Privacy Laws 2020	Emphasizes fragmentation and uneven enforcement of data privacy laws globally.
Lyon, D.	2014	Surveillance, Snowden, and Big Data	Discusses the consequences of mass state surveillance on civil liberties.
European Commission	2018	GDPR Implementation Report	Evaluates the GDPR’s impact on transparency and data control among users.
UNHRC	2022	Right to Privacy in the Digital Age	Urges states to adopt human rights-based approaches to digital policy-making.

All these studies give us a general understanding that there is an urgent need to bring alignment among technological advancement, ethical governance, and enforcement of humanity. Although frameworks such as the GDPR have made great strides in institutionalizing privacy, huge gaps still remain in global harmonization and enforcement. This literature maintains the necessity of ongoing research, into new technologies and emerging digital practices, especially for this day and age.

Objective of the Study

The purpose of this research is to provide a critical understanding of data protection frameworks, which are emerging increasingly as a means for the protection of human rights in a digital environment. The research, therefore, looks into the legally, ethically, and ftechnically challenging terrains involved with data-driven governance and corporate practices. It, therefore, seeks to appraise the impact of existing legal mechanisms-especially the GDPR and India's DPDP Act-in protecting individual freedoms in light of persistent and grave challenges such as surveillance, algorithmic bias, and digital exploitation. The study hopes to generate balanced, inclusive, and futuristic policy recommendations that prioritize the protection of human dignity without hindering technological innovation by analyzing regulatory gaps, international case studies, and ethical dilemmas.

2.1. Research Questions

This review examines the relationship between data protection and human rights in the digital era, focusing on how existing laws address the challenges arising from rapidly evolving digital technologies and their implications for fundamental human rights. It examines how state surveillance mechanisms and corporate data practices may infringe on privacy, personal autonomy, and protection against discrimination. The review also evaluates the effectiveness of international legal frameworks, particularly the General Data Protection Regulation (GDPR), in safeguarding cross-border data privacy and promoting transparency and accountability among data controllers. It also explores the ethical and legal foundations for a globally coherent digital governance model.

3. Understanding Data Protection and Human Rights

The interplay between data protection and human rights has become one of the most pressing legal and ethical issues of the digital age. In order to appreciate the complexities of this relationship, it is essential to define core concepts, trace the development of data protection legislation, and examine the broader implications for fundamental rights in digitally mediated environments.

3.1. Definitions of Key Concepts

Data privacy is the individual's right to control their personal information, ensuring autonomy and protection from unauthorized surveillance or exploitation, and is a subset of the broader right to privacy enshrined in the UDHR and ICCPR [12].

Personal data, as defined by GDPR, includes information about an individual's physical, physiological, genetic, mental, economic, cultural, or social identity, and has expanded significantly with the rise of digital technologies [13].

Digital Rights encompass human rights in digital technologies, including privacy, freedom of expression, information access, and data ownership, promoting liberty, dignity, and fairness in both virtual and physical domains [14].

3.2. Evolution of Data Protection Laws

The evolution of data protection legislation has followed closely along the development of technology and the growing awareness of privacy risks by society. Early data protection efforts were a reaction to the automated handling of personal records in the 1970s. In 1973, Sweden implemented the first comprehensive data protection statute, followed by Germany and France in the 1970s too. The OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data (1980) represented the first serious attempt at--International harmonization of principles [15]. The important milestones in data protection legislation evolution are illustrated in Figure 1.

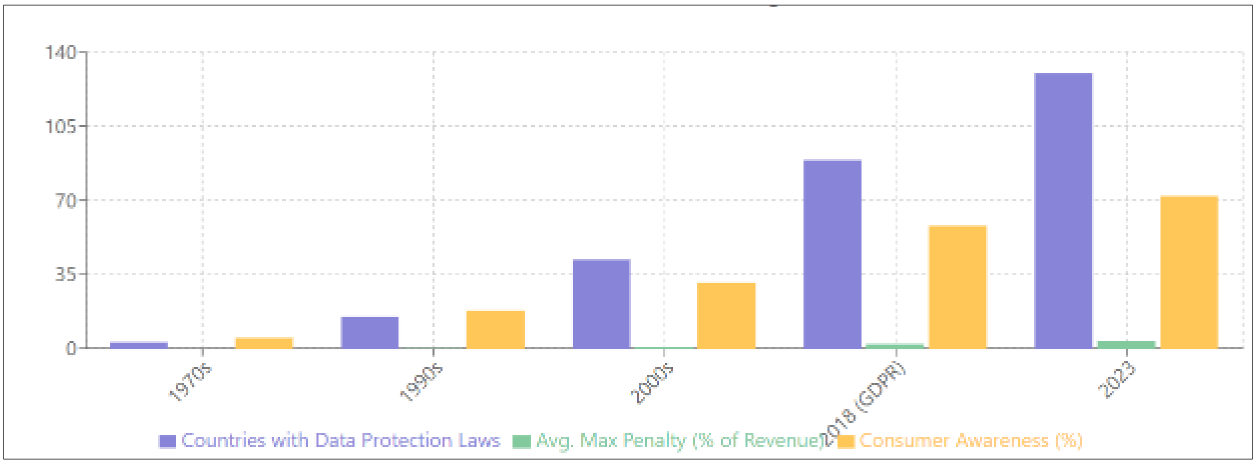

Figure 1 Data Protection Evolution [15].

The European Union Data Protection Directive (95/46/EC) was adopted in 1995 and laid down by the General Data Protection Regulation (GDPR) in 2018. As manifested in its principles for transparency, accountability, purpose limitation, and data minimization, the GDPR has set a global standard. Other major techniques including consent, the right to be forgotten, and data portability were defined. Other jurisdictions followed suit, although often with substantial differences in the scope and enforcement of the measures. Below, Table 2 enumerates major milestones in the evolution of data protection law by regions.

Table 2 Milestones in the Global Evolution of Data Protection Laws

Year	Legislation / Framework	Jurisdiction	Significance
1973	Data Act	Sweden	First national data protection law.
1980	OECD Privacy Guidelines	OECD Member States	First international framework; emphasized fair information principles.
1995	EU Data Protection Directive (95/46/EC)	European Union	Harmonized data laws in the EU; precursor to GDPR.
2000	Safe Harbor Agreement	US–EU	Allowed data transfers under specific safeguards (later invalidated).
2011	Personal Data Protection Act	Singapore	Set sectoral obligations for private data controllers.
2016	GDPR Adopted	European Union	Global benchmark for data protection; includes extraterritorial scope.
2018	California Consumer Privacy Act (CCPA)	United States (California)	First U.S. state law with GDPR-like provisions.
2023	Digital Personal Data Protection Act	India	Establishes rights-based data governance with consent and penalty mechanisms.

There is now a significant advancement in the global scenario of data protection, but it is still disjointed. In several countries, there might not be adequate legislation to address privacy issues, as well as divergent enforcement mechanisms, sovereignty norms in data ownership, and cultural interpretations of privacy that provide challenges to creating a cohesive international framework. [16].

3.3. Human Rights Implications in Digital Environments

Digital technology has transformed the ways in which human rights are experienced, exercised, and violated. While digital technology offers opportunities for access to education, healthcare, and expression, it also creates serious threats to the individual-from digital surveillance and behavioral manipulation to algorithmic profiling and data-based discrimination. These developments pose serious implications for the following basic rights:

3.3.1. Right to Privacy

The right of the individual to be left alone is being violated with pervasive surveillance systems implemented by biometric tracking and AI-powered camera systems. Surveillance has shifted-I state will watch you-to the private corporations that are harvesting user data to profit commercially. [17]

3.3.2. Freedom of Expression and Access to Information

Wherein the filtering of content and data algorithmically creates echo chambers, it may also suppress dissenting voices. If the user is profiled unjustly, this may create conditions for self-censorship because of fear of surveillance [18].

3.3.3. Equality and Non-discrimination

Equality and Non-Discrimination: AI systems trained on biased data sets can replicate and heighten social inequalities. Predictive policing, credit scoring, and recruitment algorithms have shown discriminatory outcomes that are race-, gender-, or socioeconomic status-based. [19]

3.3.4. Autonomy and Informed Consent

Digital platforms often bury data collection practices under pages of impenetrable legalese and lengthy privacy policies, paired with default settings to dissuade genuine consent. Complex terms may allow the users to unconsciously give away their rights, thanks to differential power dynamics. [20]

For all of the above, protection of human rights in digital environments is no longer an option but a must. Authorities such as the United Nations Human Rights Council (UNHRC) have argued that a human-rights-based approach must be adopted by states to develop online policies that respect, protect, and fulfill individuals' freedoms. This will require careful navigation between law, ethics, and technology, ensuring that technological progress does not undermine fundamental freedoms [21].

4. Legal and Regulatory Frameworks

Due to the increased speed of the deployment of digital technologies and the multitude of risks that those technologies pose to personal data and to fundamental rights, respective legal and regulatory frameworks are emerging all over the world. This set of laws would aim at carving out a balance between innovation and personal autonomy; ensuring accountability to the manner in which data is handled; and achieving harmonization across borders in governance on digital issues. From the all-embracing General Data Protection Regulation (GDPR) in the European Union to emerging legislation in India and the United States, the global legal landscape varies from one jurisdiction to another and reflects distinct approaches based on their respective constitutional values, economic priorities, and cultural understanding of privacy and human rights. To make comparisons easier, the following Table 3 presents all the important data protection frameworks and human rights, such as scope, principles, and alignment.

Table 3 Comparative Overview of Key Data Protection and Human Rights Frameworks

Framework	Jurisdiction	Key Features	Human Rights Alignment
General Data Protection Regulation (GDPR)	European Union	Comprehensive; applies extraterritorially; includes consent, data minimization, right to erasure, DPIAs.	Strong emphasis on Article 8 (Right to data protection) of the EU Charter of Fundamental Rights.
California Consumer Privacy Act (CCPA)	California, USA	Consumer-focused; gives rights to know, delete, opt-out of sale; lacks requirement for explicit consent.	Recognizes privacy as a consumer right; limited alignment with international human rights norms.
Digital Personal Data Protection Act (DPDPA)	India	Consent-centric; cross-border data transfer conditions; penalties for breaches; right to grievance redressal.	Emerging rights-based model inspired by GDPR but tailored to Indian context; enshrines user-centric principles.
Convention 108+	Council of Europe	First binding international treaty; includes accountability, purpose limitation, cross-border protections.	Reinforces right to privacy as fundamental; integrates modern digital rights into a treaty framework.
OECD Privacy Guidelines (2013 update)	OECD Member States	Non-binding; focuses on data quality, transparency, security safeguards, accountability.	Promotes foundational principles, but lacks enforcement; considered a soft law approach to digital rights.
Universal Declaration of Human Rights (UDHR)	United Nations	Article 12 protects against arbitrary interference with privacy, home, or correspondence.	Serves as the normative basis for digital privacy as a universal right in international law.
International Covenant on Civil and Political Rights (ICCPR)	United Nations	Article 17 mandates legal protection against data misuse and surveillance.	Enforces global obligations on states to respect digital privacy and data rights in digital ecosystems.

The frameworks under review show different levels of maturity with regard to data protection. GDPR is the most comprehensive of them, promoting transparency and user control. The CCPA stipulates consumer rights, while India's DPDPA seeks a compromise between global standards and local needs. Instruments like the Convention 108+ and the OECD Guidelines promote international co-operation in crossing borders with data protection, but often lack the power of legal enforcement.

5. The Role of Technology in Privacy Infringement

The stunning advancements in technology have completely transformed modernity, but they have equally imposed complicated threats on individual privacy and autonomy. Artificial Intelligence (AI), machine learning, big data analytics, the Internet of Things (IoT), and biometric surveillance have facilitated more extensive and intensive collection of personal data. These technologies improve efficiency and offer personalized services; however, they open up new avenues for privacy violations and surveillance by the state or corporate entities. The blend of these technologies into daily living poses serious impediments to striking a balance between innovation and human rights [22]. Figure 02 presents the technological mechanisms that trigger privacy violations within the digital ecosystem as well as the interdependencies among them, contrasting against the backdrop of data profiling and surveillance.

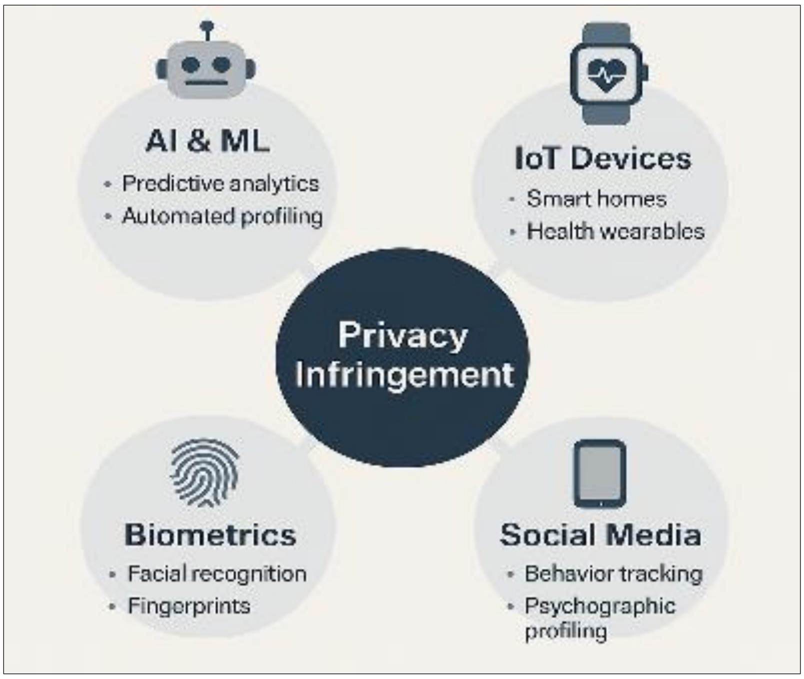

Figure 2 Technological mechanisms driving privacy breaches through data profiling and surveillance [22]

5.1. Artificial Intelligence, Machine Learning, and Big Data Analytics

AI and ML exploit vast datasets to make predictions, automate decisions, and improve their performance. Big data analytics operate by aggregating personal information from different sources in order to find trends. Yet these functions can create biases, increase opacity, and infringe upon privacy rights and rights of parity. For example, predictive policing instruments target vulnerable populations based on biased datasets [23]. The obscuring nature of the algorithms raises many concerns about accountability and fairness, especially in highly sensitive areas such as criminal justice, health, and finance [24].

5.2. Internet of Things (IoT) and Smart Devices

These IoT devices that have revolutionized homes and public infrastructure include smart home assistants and fitness trackers, effectively converting them into data-generating systems. The lack of strong encryption technologies that characterize these systems makes such installations vulnerable to breach and unauthorized surveillance [25]. In fact, many IoT systems perform data collection and transmission with little or no user awareness or consent, integrating information about users through passive sensors [26].

5.3. Facial Recognition and Biometric Surveillance

Facial recognition technology (FRT) and biometric data collecting systems are rapidly being deployed in the public and private sectors, including law enforcement and identity verification. Dangers of mass surveillance, misidentification, and racial bias are still hotly debated [27]. Unalterable once breached, biometric data adds fuel to deliberations on data security and ultimate human rights [28]. A spate of examples illustrate that facial recognition systems are prone to disproportionately misidentify members of minority communities, potentially leading to wrongful accusations and violations of their rights [29].

5.4. Social Media and Behavioral Profiling

Social media platforms engage in extensive behavioral tracking to enhance user engagement and target lucrative ads. Such systems often create psychographic profiles that can be sold to third parties for purpose manipulation, creation of filter bubbles, and even election interference [30]. Nontransparent privacy policies and vague terms to data ownership get in the way of user control over their personal data and create a gray area between what can be called voluntary sharing versus invasive extraction of data [31].

6. Ethical Dilemmas and Human Rights Challenges

Increased digitization raises significant ethical problems with respect to boundaries of surveillance, autonomy of algorithms, transparency of data, and fairness. The interplay between progress in technology and human rights is becoming increasingly complex. Here, we will explore primary ethical questions through structured comparison tables which examine different dimensions of each issue.

6.1. Balancing National Security and Privacy

Governments across the world claim that national security is the basis for invasive data practices. Nonetheless, without sufficient legal and institutional safeguards, operations can spiral into mass surveillance, chilling effects on freedom of expression, and disproportionate targeting of some communities [32]. The post-9/11 security environment witnessed the promulgation of widespread surveillance legislation like the USA PATRIOT Act, which has drawn considerable fire for lack of oversight and overreach [33]. Globally, there continues to be debate around how to ensure that surveillance is both proportionate and necessary while respecting individual rights [34]. Table 4 below compares this tension across some core elements, including justification, oversight, and impact on human rights.

Table 4 Tension between national security measures and individual privacy rights

Aspect	National Security Emphasis	Privacy Rights Emphasis
Justification	Protection from terrorism, cyber threats, and criminal acts	Preservation of civil liberties and personal freedom
Data Collection	Bulk metadata collection, surveillance programs	Targeted collection with user consent
Oversight Mechanism	Often classified or executive-led	Requires judicial or legislative oversight
Public Awareness	Limited, due to secrecy laws	Promoted via transparency policies and media exposure
Risk Trade-off	Risk of overreach and false positives	Risk of delayed response to emerging threats

6.2. Algorithmic Bias and Discrimination

Algorithms can unintentionally replicate social inequalities when trained on biased datasets. This creates real-world harm, especially in automated decision-making systems which is discussed inTable 5.

Table 5 Comparative analysis of algorithmic bias across sectors and its impact on human rights

Sector	Source of Bias	Human Rights Impact	Ethical Challenge
Criminal Justice	Historical policing data	Racial profiling, unjust risk scoring	Unequal treatment under the law
Hiring and Recruitment	Gender-imbalanced historical hiring data	Discrimination against women and minorities	Violates right to equal opportunity
Healthcare	Uneven medical records across groups	Misdiagnosis or under-treatment of minorities	Inequity in access to healthcare
Financial Services	Socio-economic data biases	Loan denial to marginalized groups	Inequality in credit access

7. Toward a Balanced Approach

As the digital landscape continues to evolve rapidly, the pursuit of a fair and ethical data governance framework becomes paramount. Balancing the protection of personal data with the safeguarding of fundamental human rights requires a multidimensional approach—rooted in legal reforms, technological responsibility, individual empowerment, and global cooperation.

7.1. Principles of Ethical Data Governance

An adequate data governance paradigm requires the underpinnings of ethics-for example-fairness, transparency, accountability, and purpose limitation [35]. These principles happen to correspond with those rights-based frameworks-most notably the EU's General Data Protection Regulation (GDPR) which mandates lawful, fair, and transparent data processing [36]. Ethical governance encourages minimization of data collection and treating people whose data is processed as rights-holders and not just mere data points. The individual's understanding of what is being done in his data processing creates trust and compliance [37].

7.2. Privacy by Design and by Default

Privacy by design and privacy by default should not be reactive but proactive strategies. For those requiring that privacy be embedded into the architecture of systems at the beginning and defaults set to favor protection of users, [38] it is essential for secure coding practices, access limitations, and encryption, but systems should only collect the minimum necessary information. These principles have been institutionalized into the GDPR and have since been accepted worldwide as best practices [39].

7.3. Empowering Individuals Through Digital Literacy and Rights Awareness

Digital literacy is the key to empower people against manipulation, profiling, and the loss of privacy. A public campaign, simplified privacy interfaces, and education would be necessary as many still do not know they should demand their data rights [40]. Studies show the more literate ones become, the stronger their demand for transparency and ethical design. Hence, this would further enforce democratic accountability in digital governance [41].

7.4. Cross-border Data Flow and International Cooperation

Cross-nationally, the phenomenon of data transfer raises unique challenges due to the fact that such movements are subject to different standards in different countries. Thus, without any harmonization of rules, inconsistent enforcement would have created gaps between protections [42]. Major international organizations have been championing the cause of the OECD and the UN for multilateral agreements and cooperative enforcement as a means of achieving global standards of innovation and rights protection [43]. An example of this is the OECD's Privacy Guidelines, which contain principles guiding interoperability and trust in global digital economies [44].

8. Future Directions and Recommendations

8.1. Enhancing Accountability of Technology Companies

Tech companies especially those operating at a multinational level—are one of the biggest collectors of user data and exert considerable power over both private and public spheres. Corporate accountability must therefore be improved to ensure that data collection and usage remain ethically and rights-compliant. These could include solid regulatory oversight, mandatory transparency reports, third-party audits, and the potential for rigorous penalties for those who are caught breaking these laws. Companies may also be required to create internal data ethics boards and do impact assessments, which evaluate the effects of a particular service on different stakeholders, prior to the rollout of any service that engages huge amounts of user data. Aligning corporate incentives with ethical outcomes signals to regulators how to bring about a culture where data protection is embedded in business models rather than considered an afterthought. Table VI maps the comparative accountability frameworks against which different jurisdictions regulate technology companies.

Table 6 Comparative Overview of Corporate Accountability Mechanisms for Data Protection

Jurisdiction	Key Accountability Mechanisms	Enforcement Body	Effectiveness
EU (GDPR)	Data Protection Impact Assessments, Fines, Reporting	European Data Protection Board (EDPB)	High
USA (CCPA/FTC)	Transparency Reports, Civil Penalties	Federal Trade Commission	Moderate
India (DPDP Act)	Consent Manager Role, Grievance Redressal Mechanism	Data Protection Board of India	Evolving
Canada (PIPEDA)	Accountability Principle, Compliance Programs	Office of the Privacy Commissioner	Moderate

8.2. Promoting Public-Private Partnerships for Ethical Technology

PPP is a collaboration platform to ensure that technological development is ethical. Governments, academia, and industries must join hands to make technologies to protect rights rather than be in violation of them. Examples of PPP collaborations include jointly convened research projects, co-branded ethical AI development labs, and regulatory sandboxes where tests are done with innovative technologies in a guided framework. PPP is essential for setting guidelines for certificate-related ethical standards for emerging technologies so that responsibly developed Artificial Intelligence and facial recognition systems come to the forefront. By encouraging these partnerships, stakeholders will share their expertise, resulting in more inclusive and responsible technology ecosystems.

8.3. Research Gaps and Future Studies

While the number of works relating to data protection and digital rights has grown in recent years, there are several gaps in the investigation. The empirical information is scant as to how specific communities, especially marginalized or vulnerable groups, are disproportionately subjected to digital surveillance and algorithmic bias. Additionally, the long-term psychological and sociopolitical impacts of data commoditization need to be thoroughly investigated. Future studies probably necessitate interdisciplinary approaches and need to factor in fields of law, technology, ethics, and sociology. Research also needs to evaluate novel technologies for effective protection of privacy, such as differential privacy and federated learning, in real-life scenarios. With the understanding of these voids and addressing them, scholars and policymakers would work toward a more nuanced and inclusive digital rights framework.

9. Conclusion

The digital age has brought to the forefront issues regarding data protection and human rights. Today such data can be misused as a valuable commodity. With that, misuse of data brings severe threats like violations of privacy, dignity, and individual autonomy. Although documents like GDPR, CCPA, and India's Digital Personal Data Protection Act seem to reflect progress in data rights, they also stress the need for a balanced global approach. Emerging technologies such as AI, big data, IoT, and biometrics often reside in ethically muddled waters and raise fundamental questions about human rights, especially concerning the vulnerable: Ethical dilemmas of national security, algorithmic bias, and known consent necessitate emphasis on privacy by design principles in digital infrastructures. In short, a balanced approach to innovation-rights advancement must be multi-stakeholders' strategy based on ethical governance, international cooperation, corporate accountability, and user empowerment. Education and digital literacy are imperative for one to understand and claim his or her rights over data. Future studies should delve into how power manifests in data ecosystems and the future social-political implications of digitized surveillance. Data privacy protection should be both legal and, more importantly, moral, keeping democratic values alive, building trust for technology, and enabling equity in digital transformation.

References

[1] Gstrein, O. J., and Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy and Technology, 35(1). https://doi.org/10.1007/s13347-022-00497-4

[2] Teo, S. A. (2024). Artificial intelligence and its 'slow violence' to human rights. AI and Ethics. https://doi.org/10.1007/s43681-024-00547-x

[3] Eke, D., and Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. Deleted Journal, 3(1). https://doi.org/10.1007/s44206-024-00101-6

[4] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., and Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

[5] European Commission. (2018). GDPR implementation report. Brussels: European Commission.

[6] Greenleaf, G. (2020). Global data privacy laws 2020: 10 global trends. Journal of Law, Information and Science, 26, 1–19.

[7] Lyon, D. (2014). Surveillance, Snowden, and big data. Big Data and Society, 1(2). https://doi.org/10.1177/2053951714541861

[8] Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560. https://doi.org/10.2139/ssrn.667622

[9] Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(2), 203–218.

[10] United Nations Human Rights Council. (2022). The right to privacy in the digital age. Geneva: United Nations.

[11] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.

[12] Singh, J., and Cobbe, J. (2019). The security implications of data subject rights. IEEE Security and Privacy, 17(6), 21–30. https://doi.org/10.1109/msec.2019.2914614

[13] Graeden, E., Rosado, D., Stevens, T., Knodel, M., Hendricks-Sturrup, R., Reiskind, A., Bennett, A., Leitner, J., Lekas, P., and DeMooy, M. (2023). A new framework for global data regulation. arXiv. https://doi.org/10.48550/arxiv.2308.12955

[14] Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005. https://doi.org/10.1016/j.jrt.2020.100005

[15] Mantelero, A. (2018). AI and big data: A blueprint for a human right, social and ethical impact assessment. Computer Law and Security Review, 34(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

[16] Salgado-Criado, J., and Fernandez-Aller, C. (2021). A wide human-rights approach to Artificial Intelligence regulation in Europe. IEEE Technology and Society Magazine, 40(2), 55–65. https://doi.org/10.1109/mts.2021.3056284

[17] Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., and Busch, C. (2020). Demographic bias in biometrics: A survey on an emerging challenge. IEEE Transactions on Technology and Society, 1(2), 89–103. https://doi.org/10.1109/TTS.2020.2992344

[18] Gomez, J. F., Machado, C. V., Paes, L. M., and Calmon, F. P. (2022). Algorithmic arbitrariness in content moderation. IEEE Transactions on Technology and Society, 3(1), 45–58. https://doi.org/10.1109/TTS.2022.3145678

[19] Leslie, D. (2020). Understanding bias in facial recognition technologies. IEEE Technology and Society Magazine, 39(2), 40–47. https://doi.org/10.1109/MTS.2020.2992345

[20] Hildebrandt, M. (2021). A wide human-rights approach to Artificial Intelligence regulation in Europe. IEEE Transactions on Technology and Society, 2(3), 120–130. https://doi.org/10.1109/TTS.2021.3098475

[21] Mantelero, A. (2018). AI and big data: A blueprint for a human right, social and ethical impact assessment. Computer Law and Security Review, 34(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017

[22] Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

[23] Barocas, S., and Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732. https://doi.org/10.2139/ssrn.2477899

[24] O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Crown Publishing.

[25] Haddadi, H., Howard, H., Chaudhry, A., and Crowcroft, A. (2018). Privacy risks in IoT: A review. IEEE Internet Computing, 22(6), 25–33. https://doi.org/10.1109/MIC.2018.2872086

[26] Ziegeldorf, K., Morchon, O. G., and Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. Security and Communication Networks, 7(12), 2728–2742. https://doi.org/10.1002/sec.795

[27] Garvie, R., Bedoya, A., and Frankle, N. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy and Technology.

[28] Jain, S., Kumar, A., and Nandakumar, K. (2017). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2017, Article 41. https://doi.org/10.1186/s13634-017-0451-3

[29] Buolamwini, J., and Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

[30] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.

[31] Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(1), 203–218.

[32] Lyon, D. (2015). Surveillance after Snowden. Cambridge: Polity Press.

[33] Posner, E., and Vermeule, A. (2007). Terror in the balance: Security, liberty, and the courts. Oxford University Press.

[34] United Nations Human Rights Council. (2018). The right to privacy in the digital age (A/HRC/39/29). https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age

[35] Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.

[36] European Union. (2016). General data protection regulation (GDPR) (Regulation (EU) 2016/679). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[37] Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707.

[38] Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

[39] International Association of Privacy Professionals (IAPP). (n.d.). Understanding privacy by design and by default. https://iapp.org

[40] van Dijck, J., Poell, T., and de Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

[41] European Union Agency for Fundamental Rights. (2020). Data protection and privacy: Fundamental rights survey. https://fra.europa.eu

[42] Kuner, J. (2013). Transborder data flows and data privacy law. Oxford Internet Institute.

[43] United Nations Conference on Trade and Development (UNCTAD). (2016). Data protection regulations and international data flows: Implications for trade and development. https://unctad.org

[44] Organisation for Economic Co-operation and Development (OECD). (2013). OECD guidelines on the protection of privacy and transborder flows of personal data. https://www.oecd.org