SCIENTIFIC CULTURE, Vol. 12, No. 5, (2026), pp. 989-990
Open Access. Online & Print
www.sci-cult.com
DOI: 10.5281/zenodo.20721040

DATA PROTECTION LAWS AND DIGITAL CULTURE: A COMPARATIVE REVIEW OF GLOBAL REGULATORY FRAMEWORKS, TECHNOLOGICAL ETHICS, AND HUMAN-CENTRED GOVERNANCE

Dr. Shweta Gupta[1], Dr. Sandeep Kumar[2], Pritam Kumar Ghosh[3], Jagadeesh Sundaramoorthy[4], Priyanka Nair[5], Dr. Pawan Kumar[6]

[1]Assistant Professor, Affiliation Address/ College Name: GLA University, Mathura, Email id: Gupta.shweta.1984@gmail.com
[2]Assistant Professor, Name of institution - Faculty of Legal Studies, Motherhood University Roorkee Uttarakhand. Email id - behappysk9@gmail.com , Orchid id - https://orcid.org/0000-0002-9432-4510
[3]Assistant Professor, Department- School of Law, University- Christ (Deemed to be) University, Bangalore Email ID- pritamkumar.ghosh@christuniversity.in , ORCID ID- 0000-0001-7845-6129
[4]Tecnical Architect, Department: US Digital Transformation, Company Name: Infosys Ltd Location: Raleigh, NC, United States of America. Email ID: s.jaga87@gmail.com , ORCID ID: 0009-0000-1012-2034
[5]Research Scholar, University-Hidayatullah National Law University, Raipur Email ID -priyanka2223@hnlu.ac.in , Orcid id- 0009-0002-6995-5940
[6]Assistant Professor, Affiliation Address: College of Law & Legal Studies, Teerthankar Mahaveer University, Moradabad. Email Address: Pawankumar.law@tmu.ac.in , ORCID - 0009-0003-1983-0370

Abstract
Personal data is a key aspect of digital culture, influencing online identity, social engagement, institutional trust, and technology-mediated governance. Data protection laws are not only legal but also ethical; with the rise of artificial intelligence, biometric systems, platform economies and cross-border data flows, data protection laws are becoming more relevant than ever. This review sought to analyze the development of data protection legislation by making a comparative study of the laws in the world, focusing on digital culture, technological ethics, AI governance, and human rights. A comparative systematic narrative review approach was used, using legal instruments, policy documents, regulatory guidelines and interdisciplinary academic literature. The major frameworks considered were the EU GDPR, UK GDPR, California CCPA/CPRA, Brazil LGPD, India's Digital Personal Data Protection Act, China's PIPL, South Africa's POPIA, the OECD privacy principles, the Convention 108+ of the Council of Europe and various UN and UNESCO instruments. The review identified a convergence of data protection laws across the world, with a focus on transparency, consent, accountability, individual rights and institutional responsibility, and a divergence in how these laws are enforced, digital sovereignty, access by the state, regulation of AI and cultural understanding of privacy. The article adds by suggesting data protection as a legal, ethical, cultural and governance framework for trustworthy, inclusive and human-centred digital transformation.

Keywords: *Data protection laws; digital culture; privacy regulation; technological ethics; human-centred governance; AI governance; global regulatory frameworks; digital rights; algorithmic accountability; data sovereignty.*

1. Introduction

The personal data is now one of the most important resources of the modern digital culture. The utilization of data-driven platforms has now expanded into routine areas such as, communication, shopping, teaching, health care, banking and civil life. Artificial Intelligence (AI), biometrics, and predictive analytics and automatic decisions-making processes has enhanced the power and fragility of personal data. Data protection no longer only involves avoiding privacy violations, but is instead a central issue for digital participation, institutional credibility, social identification and the responsible development of technology.

This broader shift is reflected in the development of data protection laws. Initial privacy issues were more related to intrusion and unauthorised exposure. In today's digital world, however, privacy has grown into a wider concept of autonomy, dignity, fairness, transparency, accountability and human agency. The processing of large amounts of personal data has led to risks of surveillance, manipulation, discrimination, profiling, exclusion and loss of control over digital identity. These risks are particularly important in algorithmic systems where decisions could be taken based on black-box processing. Thus, data protection laws now govern not only the use of data but also the power dynamics among people, corporations, states, and digital infrastructures. The legal autonomy and distinctiveness of data protection has also been identified as separate from general privacy, in the EU legal order, for instance, where data protection is a distinct fundamental rights framework (Lynskey, 2014).

To address these issues, there have been the development of global regulatory frameworks, which vary in terms of their orientation, scope and enforcement. The EU General Data Protection Regulation (GDPR) created a rights-based approach that puts the emphasis on lawfulness, fairness, transparency, purpose limitation, data minimisation, accountability, and enforceable rights of individuals (European Parliament and Council of the European Union, 2016). Other jurisdictions evolved strategies influenced by local legal culture, market systems, political ideologies, and cultural expectations. These disparities illustrate that data protection is also a cultural and ethical reflection of societies' concepts of personhood, trust, freedom, security and responsibility in digital life.

This article falls under the category of digital culture, technological ethics, AI and society, social sciences, and human-centred innovation. These spheres are relevant as data protection principles provide the framework that governs people's interaction with the digital world, shapes the generation of trust in institutions and affects the values promoted or questioned in technologies. The regulation of data governance and privacy has implications for digital citizenship, platform accountability, social inclusion and democratic participation in data driven societies. Moreover, the importance of technological development and alignment with human rights, inclusion, equity, fairness, transparency and accountability have become central in international discussions about ethics in AI (UNESCO, 2021).

The core argument of this review revolves around the fact that a large number of discussions about the area still largely legalistic, institution-based or jurisdiction-based. Although this is an important dimension, it fails on its own to explain the influence of data protection law on the area of digital culture, technological ethics, algorithmic accountability, social trust and human-centred governance. Simply adopting a legal perspective neglects the cultural dimensions of privacy, the ethical considerations that may be attached to the acquisition of data, and the social implications of computer-generated outputs. After all, not only do the notion of privacy consists of the ideas of secrecy and consent, there is also a tight relationship between the former and the expectations, norms and data flows associated with the particular context (Nissenbaum, 2004). Hence, an interdisciplinary review is needed.

Therefore, this article reviews and compares globally how data protection laws have been developing, and how relevant they are for digital culture, technology ethics, and human-centric governance. It traces the history of data protection laws in the digital transformation era, the similarities and differences of main international instruments, their views on AI, profiling, surveillance and platform governance, ethical and human values which are embedded into these laws, and the governance framework that needs to be ensured in order for data protection to be human-centric in the future. Value proposition: this article connects the area of law with digital culture, AI ethics, human values, and comparative governance in a common framework that can promote trustworthy, equitable, and human-centric digital society.

2. Conceptual Background and Literature Review

2.1 Conceptual Evolution of Privacy and Data Protection

The concept of privacy initially served the purpose of protecting one from unwanted physical or social intrusion, and later developed into a broad legal and ethical notion linked to personal autonomy, dignity, identity and control over information. As initial privacy research interpreted privacy as "the right to

be let alone" or the right to conceal personal information, contemporary data protection scholarship centers on organized acquisition, use, transfer and profiling of personal data within digital spaces (Warren & Brandeis, 1890). The Convention 108 was an early binding international response to automatic processing of personal data, which was institutionalised under the Convention (Council of Europe, 1981). The privacy harms went beyond secrecy to concerns about information collection, processing, dissemination and invasion (Solove, 2006).

2.2 Datafication and Digital Culture

Datafication transformed digital culture by turning social behavior, communication, consumption, mobility, education, and governance into quantifiable and monetisable data. Digital platforms emerged as infrastructures for predicting behaviour, sorting social groups, constructing identities, and making decisions in institutions. In this context personal data was a cultural resource that organized power, participation, visibility and vulnerability. Everyday digital activities were turned into predictive products that would influence the economy and behavior, as surveillance capitalism showed (Zuboff, 2015). Similarly, big data ethics scholarship cautioned that large-scale analytics could lead to new power imbalances and governance issues, in addition to the traditional models of individual control (Richards & King, 2014).

2.3 Technological Ethics and Human Values

The normative basis for judging whether or not data-driven systems respected human values was technological ethics. As digital systems became more prevalent in shaping social opportunities and institutional decisions, fairness, transparency, accountability, non-discrimination, proportionality, explainability, and human oversight became essential. Ethical data governance was not just about procedure and the legality of it, it was about protecting against manipulation, exclusion, opacity and power imbalance. Digital ethics, in turn, linked data protection to responsible innovation and human welfare (Floridi, 2019). A second survey of AI ethics guidelines around the world also revealed common references to the principles of transparency, justice, fairness, non-maleficence, responsibility and privacy for the responsible governance of AI (Jobin et al., 2019).

2.4 Human-Centred Governance

Human-centred governance was described as a regulatory regime that put individual rights and social justice, cultural sensitivity, ethical design and public accountability at its heart of digital regulation. It acknowledged that data governance should not be determined solely by market efficiency, technology or state control. Rather, it is meant to safeguard individuals and groups against abusive or unfair data practices. The European Data Protection Supervisor's activities on digital ethics highlighted the importance of considering dignity and human values in the context of data-driven innovation and institutional accountability (European Data Protection Supervisor, 2015).

2.5 Data Protection and AI Governance

The rise of AI intensified the relationship between data protection and algorithmic governance. Personal data was essential for automated decision making, profiling, biometric processing, predictive systems and machine learning systems, and could impact access to services, opportunities and rights. As such, AI governance needed to include measures to ensure transparency, lawful processing, impact assessment and contestability. Discussions around regulation increasingly framed data protection as a basis for trusted AI, particularly when AI-driven automation had substantial legal, social or ethical implications for people (Mantelero, 2018).

2.6 Global Regulatory Traditions

There were a number of traditions in the global data protection literature. Rights-based models focused on dignity and fundamental freedoms, consumer-protection models on notice, choice, and market fairness, sovereignty-centred models on data governance and national security, and developmental models on a balance of innovation, welfare digitisation, and citizen protection. These traditions demonstrated that the regulation of privacy was influenced by legal culture, political economy, institutional capacity and social values. The diffusion of national privacy laws was confirmed and regional differences remained significant (Greenleaf, 2019).

2.7 Research Gap

Prior research has focused on privacy law, the ethics of AI, platform governance, and global data laws. But the debate on legal, technical, cultural and ethical aspects tends to be fragmented. There has been restricted review work that has brought together global data protection frameworks, digital culture, technological ethics, human values and human-centred governance in one analytical framework. This article filled that void, placing data protection law as an ethical and cultural infrastructure for trustworthy digital societies.

3. Methodology

3.1 Review Design

The study used a comparative systematic narrative review design to explore the linkage between data protection laws, digital culture, technological ethics and human-centred governance. The choice of this design was based on the fact that it allowed the incorporation of legal texts, policy documents, regulatory guidelines and interdisciplinary research literature within a single review process. The design made it possible to do a comparative and critical description of the various data protection regimes across the world, and it provided an interpretive framework with regards to culture, ethics and governance. It also enabled the recognition of the emerging convergence and differences in the regulation of data protection across the different regimes.

3.2 Data Sources

Relevant literature and regulatory documents were collected from academic databases, legal texts and official institutional and governmental documents. Among academic databases, Scopus, Web of Science, Google Scholar, HeinOnline, SSRN, ScienceDirect, SpringerLink and Taylor & Francis were used. Among official documents sources for European Union, OECD, UNESCO, United Nations, Council of Europe, national Data Protection Authorities and official government websites were exploited. Data on the above sources were selected because they represented peer-reviewed research, primary legal documents and leading documents on the topics of privacy and artificial intelligence governance and digital rights.

3.3 Search Strategy

The search was conducted in a systematic way and a combined set of keywords regarding data protection, digital culture, ethics, AI governance and human-centred regulation was utilized. Search terms that were used included the following combinations: "data protection law" AND "digital culture"; "privacy regulation" AND "human rights"; "GDPR" AND "AI governance"; "data protection" AND "technological ethics"; "privacy law" AND "human-centred governance"; "cross-border data transfer" AND "digital sovereignty"; "algorithmic accountability" AND "data protection". Relevance of the search outcome, quality of the publication, its jurisdictional importance and alignment with the transdisciplinary nature of the article was taken into consideration while selecting suitable search outcomes.

3.4 Inclusion Criteria

The sources were included if they directly mentioned data protection regulations, privacy regulation, digital governance, technological ethics, AI accountability or human-centred digital policy. Peer-reviewed articles, official legal documents, international regulatory documents, policy reports and institutional guidelines were given priority. Studies published after 2016 were favoured as the post-GDPR era was a significant shift in privacy governance globally. Some foundational literature on privacy theory, digital ethics and human rights was also included where it was found to be necessary for the conceptual underpinning of the review.

3.5 Exclusion Criteria

Sources were excluded if they did not directly address data protection, digital culture, technological ethics or human-centred governance. Only technical cybersecurity research was excluded if it had significant privacy rights or regulatory considerations. Non-academic opinion pieces, unsupported commentaries, duplicate records, outdated legal summaries, and sources lacking in methodological and conceptual value were excluded. Descriptions of legal systems in one country were not included unless they were relevant to comparative analysis or were a significant regulatory model in the global system of data protection governance.

3.6 Selection of Regulatory Frameworks

These regulatory regimes were chosen because of their international reach, legal experience, geographical variety and suitability for digital culture and technological governance. The review focused on the EU GDPR, UK GDPR and Data Protection Act, California CCPA/CPRA, Brazil LGPD, India Digital Personal Data Protection Act, China PIPL, South Africa POPIA, Council of Europe Convention 108+, African Union Convention on Cyber Security and Personal Data Protection, and selected UN and UNESCO instruments. These frameworks were included as they play a significant role in various rights-based, consumer-focused, sovereignty-focused, regional and developmental data governance frameworks (Great Britain, 2018; Brazilian Presidency of the Republic, 2018; California Privacy Protection Agency, 2024; Government of India, 2023; People's Republic of China, 2021; South African Government, 2013; African Union, 2014; Asia-Pacific Economic Cooperation, 2015). This choice allowed for a comparison between rights-based, consumer oriented, sovereignty centred and developmental governance models. The selected frameworks are summarised in Table 1 to clarify their jurisdictional scope, regulatory orientation, and relevance to digital culture.

Table 1. Selected Global Data Protection Frameworks and Their Regulatory Orientation

Jurisdiction/Region	Law/Framework	Regulatory Orientation	Relevance to Digital Culture
European Union	GDPR	Rights-based and accountability-centred	Strengthens digital citizenship, platform accountability, and institutional trust
United Kingdom	UK GDPR/Data Protection Act	Rights-based national adaptation	Supports responsible data governance and public/private sector accountability
United States/California	CCPA/CPRA	Consumer-protection and market-oriented	Promotes consumer choice, platform transparency, and privacy control
Brazil	LGPD	Rights-oriented and GDPR-influenced	Extends rights-based privacy governance to Latin American digital systems
India	Digital Personal Data Protection Act	Developmental and consent-based	Balances personal data rights with digital public infrastructure and welfare digitisation
China	PIPL	Sovereignty-centred and state-regulated	Links personal data protection with cybersecurity, platform control, and digital sovereignty
South Africa	POPIA	Rights-oriented constitutional model	Strengthens privacy and accountability in emerging digital governance contexts
OECD	OECD Privacy Framework	Principle-based soft-law model	Supports interoperable privacy principles and cross-border data flows
Council of Europe	Convention 108+	International rights-based treaty model	Promotes shared human-rights-based data protection standards
African Union	Cyber Security and Personal Data Protection Convention	Regional data protection and cybersecurity model	Supports privacy protection within African digital transformation
Asia-Pacific Region	APEC Privacy Framework	Cross-border accountability model	Balances privacy protection with digital trade and data-flow interoperability

3.7 Analytical Framework

Selected sources and regulatory frameworks were examined using five interconnected dimensions: legal rights and obligations, digital-cultural implications, ethical principles, AI and automated decision-making governance, and human-centred accountability mechanisms. Such a framework enabled the review to go beyond legal compliance, and to consider data protection laws' impact on digital participation, institutional trust, platform responsibility, algorithmic transparency and social values. Comparative interpretation was used to seek commonality and contrast, to highlight strengths and gaps and to highlight culturally responsive governance and autonomy, and to highlight autonomy, dignity, fairness, accountability, and culturally responsive governance.

4. Comparative Thematic Analysis

4.1 Evolution of Data Protection Laws Across Generations

Data protection laws evolve from earlier problems of privacy to complex system of governance for digital societies. Initial thought about privacy was persons' protection from intrusion, and later thought about automated databases, Internet, data

flows over borders, and profiling using algorithms. GDPR was a turning point because rights, responsibility, and enforcement were strongly established. Beyond compliance with the law, data protection is becoming about creating trustworthiness, integrity, and ethical technology and human-centric governance in the era of AI (European Parliament and Council of the European Union, 2016).

4.2 Comparative Overview of Global Frameworks

International data protection practices were shaped by divergent legal cultures, political ideas, and cultural anxieties. Europe relied on rights-based and institutionally accountable arguments, America concentrated on consumer privacy and sectoral regulation. Brazil and South Africa adopted rights-based models of data protection grounded on international privacy ideas; China intertwined the protection of personal data with ideas about digital sovereignty and state governance. Disagreements showed that data protection was not monolithic, but was rather a product of regional histories, market arrangements, collective desires, and forms of governance (Greenleaf, 2021). Table 2 presents a concise comparison of major regulatory themes across selected data protection frameworks.

Table 2. Concise Comparative Matrix of Global Data Protection Frameworks

Framework	Core Protection Focus	AI/Profiling Treatment	Cross-Border Data Approach
EU GDPR	Strong individual rights, accountability, transparency, and lawful processing	Recognises automated decision-making and profiling safeguards	Strict adequacy, safeguards, and contractual transfer mechanisms
UK GDPR/Data Protection Act	GDPR-based rights, accountability, and national regulatory control	Addresses profiling, fairness, transparency, and automated decisions	Uses adequacy regulations and GDPR-style safeguards
CCPA/CPRA	Consumer choice, transparency, opt-out rights, and sensitive data control	Emerging regulation of profiling and automated decision-making	No GDPR-style international transfer regime
Brazil LGPD	Rights-based processing, consent, accountability, and transparency	Provides review rights for automated decisions	Allows transfers through adequacy, safeguards, consent, or legal grounds
India DPDP Act	Consent, notice, data fiduciary duties, and grievance redressal	Applies generally to digital personal data but lacks detailed AI-specific provisions	Permits transfers except to restricted countries
China PIPL	Personal information rights, sensitive data protection, and state oversight	Regulates automated decision-making and unfair differential treatment	Strong state-controlled transfer mechanisms
South Africa POPIA	Accountability, lawful processing, and data subject participation	Protects against harmful solely automated decisions	Allows transfers where adequate protection or legal conditions exist
OECD Privacy Framework	General privacy principles and individual participation	Relevant through accountability and purpose-limitation principles	Supports privacy-protective international data flows
Convention 108+	Human-rights-based data protection and independent supervision	Addresses automated processing through safeguards and transparency	Promotes transborder data flows with appropriate protection

Framework	Core Protection Focus	AI/Profiling Treatment	Cross-Border Data Approach
African Union Convention	Cybersecurity, personal data protection, and national authority development	Limited direct AI provisions but relevant to digital processing safeguards	Depends mainly on domestic implementation
APEC Privacy Framework	Notice, choice, accountability, and harm prevention	Indirectly relevant through accountability and risk prevention	Supports accountable cross-border data flows

4.3 Consent, Autonomy, and the Limits of Individual Control

In platform-based digital culture, consent continued to be a key concept in data protection but its application was constrained. Users rarely read and understood privacy terms, and algorithmic systems operated in ways that were opaque, intricate, and incalculable. This reduced the autonomy of the user and transferred responsibility from the institution to the user. In these settings, consent would not be sufficient for ethical governance unless complemented by transparency, fairness, purpose limitation and increased organizational accountability (European Data Protection Board, 2020a). Big data analytics also posed threats to traditional privacy models, as it broadened the scope of secondary uses of data and reduced the impact of practical control by users (Tene & Polonetsky, 2013).

4.4 Data Subject Rights and Digital Citizenship

Data subject rights have been key to the shift from data sources to digital citizens. Rights of access, correction, erasure, portability, objection, and restriction empowered people to counter misuse and to make more meaningful contributions to digital systems. These rights also encouraged accountability by mandating that organisations explain their practices with the data. But they were only truly useful if they were accessible, known, regulated, and technologically feasible, particularly in automated decision-making scenarios where power dynamics were still unequal. (Goodman & Flaxman, 2017).

4.5 Sensitive Data, Children's Data, and Vulnerable Groups

The ethical depth of data protection laws was the protection of sensitive data, children's data and vulnerable groups. Sensitive categories, such as health information, biometric identifiers, political opinions, children's behaviour and other categories, were subject to higher protection levels, as their misuse could lead to discrimination, exclusion, manipulation or social harm. In digital culture, there was a disproportionate exposure to surveillance and profiling for vulnerable users. For this reason, special protection mechanisms were needed that would take account of dignity, dependency, age, social vulnerability and unequal bargaining power, in keeping with a human-centred approach to the regulation (United Nations Human Rights Council, 2021).

4.6 Cross-Border Data Transfers and Digital Sovereignty

Tensions between global digital integration and national regulatory sovereignty were highlighted in cross-border data transfer. International data flows were essential to the functioning of digital platforms, cloud services and multinational companies, while states wanted to shield citizens from inadequate foreign protection, surveillance threats and commercial exploitation. Various mechanisms (including adequacy decisions, contractual clauses, localization requirements and regulatory cooperation) tried to strike a balance between innovation and rights protection. In these discussions, it was established that data protection was now at the heart of digital sovereignty, geopolitical trust, and interoperability of global governance (Organisation for Economic Co-operation and Development, 2013). The Schrems II ruling also sparked a renewed discussion on international transfers of data, as it raised tensions between the foreign surveillance regime and the standards of adequacy and rights-based data protection (Kuner, 2020).

4.7 AI, Profiling, and Algorithmic Accountability

The rise of algorithmic profiling further highlighted the importance of algorithmic accountability in data protection law.Algorithmic profiling further underlined the need for algorithmic accountability in data protection law. Through opaque data processing, automated systems may be able to classify people, predict their behaviour, affect their opportunities and even perpetuate social bias. Consequently, data protection frameworks increasingly covered the topics of transparency, explainability, risk assessment, and human oversight. But there were still many laws that were

not able to effectively control complex AI systems. For a human-centred approach, the legality of profiling was not sufficient to ensure its fairness, dignity, non-discrimination and social consequences (Mittelstadt et al., 2016). The risks of relying on automated processing alone and the importance of meaningful safeguards were highlighted in the guidance on automated decision-making and profiling (Article 29 Data Protection Working Party, 2017a). Furthermore, the EU Artificial Intelligence Act suggested a move to a risk-based approach to the governance of AI systems, extending beyond data protection (European Parliament and Council of the European Union, 2024). Regulatory guidance on AI and data protection also highlighted aspects of lawfulness, fairness, transparency, accountability and lifecycle risk management (Information Commissioner's Office, 2023).

4.8 Enforcement, Institutional Accountability, and Public Trust

Effective enforcement made data protection a governance tool rather than a formal legal commitment. Institutional responsibility was enhanced by regulatory authorities, penalties, audits, data protection officers, breach notification obligations and impact assessments. Public trust relied on citizens' confidence in the accountability of organisations and governments in respect of data misuse. Lack of enforcement may result in symbolic compliance of data protection, while robust enforcement may foster responsible innovation, transparency of organisations and ethical design of public and private digital ecosystems (European Data Protection Board, 2020b).

4.9 Cultural and Ethical Values Embedded in Data Protection Laws

Data protection laws incorporated various cultural and ethical values such as dignity, autonomy, market freedom, consumer choice, public welfare, security and sovereignty. Rights-based models placed emphasis on the dignity of the individual and his/her fundamental freedoms, while consumer oriented models focused on transparency and market participation. Sovereignty-based approaches tied data governance to national control and strategic security. These differences showed that data protection was not only technical regulation but also a cultural expression of the definition of personhood, trust, power, responsibility, and ethical digital co-existence (Floridi et al., 2018). Table 3 summarises the major ethical and cultural values reflected in different data protection models.

Table 3. Ethical and Cultural Values in Data Protection Models

Data Protection Model	Dominant Value	Main Governance Concern
Rights-based model	Human dignity, autonomy, and fundamental rights	Risk of becoming overly compliance-driven without meaningful public understanding
Consumer-protection model	Individual choice, market transparency, and consumer control	Over-reliance on notice, opt-out mechanisms, and user responsibility
Sovereignty-centred model	National control, cybersecurity, and strategic data governance	Possible tension between state control, civil liberties, and independent oversight
Developmental governance model	Digital inclusion, welfare delivery, and economic innovation	Risk of surveillance, exclusion, and weak consent in rapid digitisation
International soft-law model	Interoperability, accountability, and shared privacy principles	Limited enforceability due to non-binding status
Treaty-based international model	Human rights, harmonisation, and independent supervision	Uneven ratification and implementation across jurisdictions
Platform-governance model	Transparency, accountability, and user trust	Profiling, behavioural manipulation, and concentrated platform power

Data Protection Model	**Dominant Value**	**Main Governance Concern**
AI-governance model	Fairness, explainability, and human oversight	Opaque automated systems may reproduce bias and limit contestability
Vulnerable-group protection model	Care, inclusion, safety, and social justice	General privacy rules may fail to protect children and vulnerable users
Cultural-context model	Contextual integrity and socially situated privacy	Universal rules may overlook local meanings of privacy, trust, and authority

5. Discussion

This comparative analysis indicated how data protection laws have become cultural, ethical and governance tools shaping the behavior of individuals, institutions, markets and States in digital society. Data protection is becoming about autonomy, dignity, identity, accountability and social trust in data-intensive environments where the subject leave traces online, biometric technologies, health tools, public services relying on AI.

One of the most important conclusions of the review is that there are cultural and political differences across the world in terms of conceptualization of personhood, freedom, and institutional responsibility for data protection. The European rights-based approach focuses on dignity, legality, transparency and individual control, whereas consumer-based approaches may focus on the notions of choice, notice and market fairness. The sovereignty-centred approaches link personal information governance with national security, state authority and control over digital infrastructure. The differences reflect social values and governance traditions that are embedded in data protection. Contextual integrity is helpful here as it provides an understanding of privacy as being related to social norms, roles, expectations and the flows of information in a particular context (Nissenbaum, 2004).

The results also show that the consent-based approach is becoming inadequate in complex digital ecosystems. Users of platforms are frequently faced with decision-making situations that involve information asymmetry, behavioural design, opacity of algorithms, and reliance on digital services. Consequently, formal consent is not necessarily a sign of meaningful autonomy, particularly if data is re-used, inferred, combined, processed for use for which users may not have anticipated. Cognitive constraints, design pressures, institutional power, and social expectations influence privacy behaviour (Acquisti et al., 2015). There needs to be more responsibility on organisations, developers and regulators, therefore, for human-centred data governance.

Another main question is the connection between data protection and technological ethics. AI systems, profiling tools, and predictive analytics are increasingly being used in the world of employment, credit, education, healthcare, public benefits, policing, and cultural content. If these systems are based on skewed or overabundant data analysis, they can perpetuate discrimination and exacerbate social inequities. Even if there is no intentional discrimination, big data practices can have differential effects, as algorithmic systems can be used to identify proxy variables that can mimic historical disadvantage (Barocas & Selbst, 2016). Machine learning fairness is also normative due to the fact that different definitions of fairness in machine learning can also embody different political and ethical principles (Binns, 2018).

In this conversation, it also becomes clear that data protection is a key part of public confidence in digital institutions. Citizens have greater trust in digital innovation when the law offers convincing protections against exploitation, surveillance, manipulation and arbitrary decision making. Ethical digital societies need to be accountable by design, transparent in data practices and have meaningful redress procedures. Privacy by design is significant as it makes privacy more integral to the design of the system than simply a compliance requirement added on later (Cavoukian, 2011).

Lastly, data protection governance needs to be culturally competent and interoperable on a global level. Global digital platforms are operating across jurisdictions yet there are significant variations in the expectations of privacy, institutional capabilities, and social vulnerabilities. The human-centred model should include the universal principles of dignity and fairness, as well as sensitivity to the local culture, economic and developmental context. International AI ethics documents reiterate the importance of creating governance that upholds human rights, is inclusive and that ensures that AI development is held accountable to society (UNESCO, 2021). The overall picture of data

protection laws should be seen as infrastructures of ethics, which set rules for data use, delineate power relationships and influence the human-centred digital civilisation.

6. Proposed Conceptual Framework

This review presented a Human-Centred Data Protection Governance Framework aimed at explaining how international data protection legislation can contribute to trustworthy digital culture, technological ethics and socially responsible innovation. The framework was divided into five key pillars: rights and dignity; ethical design of technology; algorithmic accountability; cultural sensitivity and social inclusion; and global regulatory interoperability. These pillars created the data protection ethical infrastructure because the modern system of data influences identity, autonomy, participation, institutional trust, and the power dynamics of the systems today.

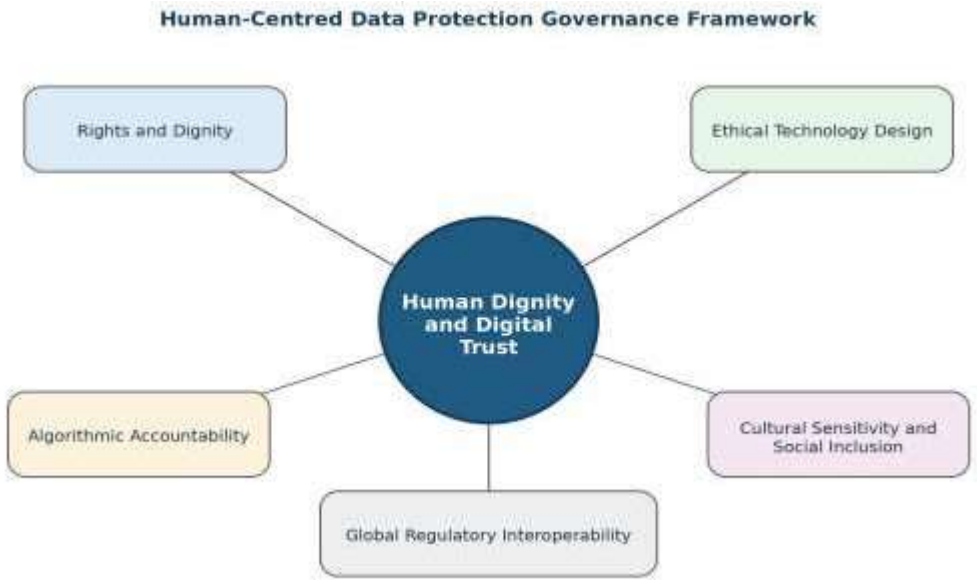

Figure 1. Human-Centred Data Protection Governance Framework

The first pillar of rights and dignity put the individual in the middle of data governance. It stressed the need for privacy and data protection to safeguard informational control, human dignity, autonomy and freedom from unwanted information surveillance or manipulation. The right to privacy has always been considered as a fundamental concern of human being; in fact, the importance has further increased as personal data has become central to the social, economic and political life (United Nations General Assembly, 1948). Data processing in this pillar was to be lawful and fair, transparent, proportionate and respectful of human agency.

The second pillar was ethical technology design, which mandates that digital systems incorporate privacy, fairness, security and transparency from the outset of their design. Ethical design integrated data protection measures into platforms, AI systems, databases, and public digital infrastructures instead of viewing data protection as a matter for compliance after the initial development. This coincided with the data protection by design and by default which mandated that organisations reduce the data they collected unnecessarily and that they implement data protection mechanisms as a default (European Data Protection Board, 2020b).

The third pillar, algorithmic accountability, discussed automated decisions, profiling, and the prediction by AI. It mandated the clear explanation, audit and justification of algorithmic systems that have an impact on rights, services and social opportunity. To ensure that automated decisions did not cause discrimination, exclusion and irresponsible data reuse (Wachter et al., 2017), accountability mechanisms were crucial.

The fourth pillar, cultural sensitivity and social inclusion, acknowledged that expectations for privacy and harms related to data may differ among communities, regions and social groups. Children, vulnerable groups, indigenous/community data, gendered privacy issues and digital inequalities should thus be included in data protection frameworks to ensure that data protection does not come at the expense of local values, social vulnerabilities and unequal access to rights.

The fifth pillar, global regulatory interoperability, focused on cooperation across jurisdictions. Rules may be disjointed, potentially resulting in reduced protection and uncertainty, given the global nature

of digital platforms, cloud systems, AI services and data flows. Convention 108+ demonstrated the possibility of international cooperation to promote common standards for personal data protection (Council of Europe, 2018). Ensuring human-centred, transparent, robust, safe and accountable AI systems was also a component of responsible digital governance, consistent with the OECD AI principles (Organisation for Economic Co-operation and Development, 2019).

7. Policy and Research Implications

The conclusions indicated that data protection laws need to go beyond mere compliance and function as tools for ethical, inclusive and people-centred digital governance. There was a need for the algorithms to be more accountable so that any profiling, biometric processing or automated decision-making based on the algorithms would be transparent, explainable and contestable. There should be privacy-by-design and ethics-by-design considerations which should be required by regulators so that protection is built-in in beforehand, not built-in after damage has occurred. Data protection impact assessment guidance also assisted in a prior assessment of sensitive data or profiling, or for large scale monitoring that could impact on rights and freedoms (Article 29 Data Protection Working Party, 2017b).

Children and their communities that are socially marginalised and vulnerable are at greater risk of being the subject of surveillance, profiling, manipulation or exclusion, and need stronger protections under policy frameworks. A culture-sensitive approach to privacy governance was also required when there are significant differences in privacy expectations, digital literacy and trust in institutions. Cooperation in respect of cross-border data flows at the global level should be enhanced by the introduction of interoperable standards, which guarantee the protection of rights and promote responsible innovation. Public engagement should also be enhanced, enabling citizens, civil society, researchers and affected communities to have an impact on decisions around data governance.

Future studies should focus on the influence of digital culture on privacy behavior, fatigue of consent, platform trust and the public perception of the rights to data. Comparative analysis should examine what is considered private, privateable, dignifying and acceptable data use in societies. There is also a need for further research on AI governance and data protection, including in the context of automated decision making, biometric surveillance, predictive analytics, algorithmic discrimination, children's digital rights, and digital economies in the Global South. Last, data justice and platform accountability should continue to be the core of scholarship moving forward; ensuring data protection benefits fairness, inclusion, democratic accountability, and human-centred digital culture.

8. Limitations of the Review

There were some limitations with this review. First, it was limited to a selection of global data protection frameworks and not every country's privacy law or regional initiative was included. Second, it was largely based on the English-language academic literature, official legal texts and policy documents, which could have restricted the scope of non-English and local perspectives on privacy and digital culture. Thirdly, data protection law is developing at a fast pace in the context of AI governance, the regulation of biometric data, cross-border data transfers, and platform accountability, among other areas. Lastly, the study was of a comparative legal-cultural nature and the results must be interpreted conceptually and analytically, not statistically and in a general sense. Empirical studies with regulators, technology developers, civil society organisations and impacted users can further contribute to this field in the future.

9. Conclusion

This review found that data protection laws have grown into more comprehensive pieces of legislation for the regulation of digital culture, technological ethics, the accountability of AI and human-focused digital societies. The comparative analysis revealed that there are a variety of differences in the legal traditions, cultural values, enforcement mechanisms, and concepts of autonomy, consent, surveillance, cross-border data flows, and algorithmic decision-making across the global regulatory landscape, but an important shared concern is that of the protection of individuals from “exploitative and opaque data practices.” Data protection has therefore come to the fore in the context of public trust, digital participation, institutional accountability and ethical technological innovations. The article brought together global regulatory frameworks, digital culture and human centred governance, thus connecting data protection with a legal, cultural, ethical, technological and human issues. In conclusion, the development of trustworthy digital societies necessitates legally sound, ethically based, culturally appropriate, transparent and dignifying data protection systems.

References

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465
2. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
3. Asia-Pacific Economic Cooperation. (2015). APEC privacy framework.
4. https://www.apec.org/publications/2015/12/apec-privacy-framework-2015
5. Article 29 Data Protection Working Party. (2017a). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. European Commission. https://ec.europa.eu/newsroom/article29/items/612053
6. Article 29 Data Protection Working Party. (2017b). Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. European Commission.
7. https://ec.europa.eu/newsroom/article29/items/611236
8. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732. https://doi.org/10.15779/Z38BG31
9. Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. Proceedings of the 2018 Conference on Fairness, Accountability and Transparency, 149–159.
10. https://proceedings.mlr.press/v81/binns18a.html
11. Brazilian Presidency of the Republic. (2018). Lei Geral de Proteção de Dados Pessoais: Law No. 13,709 of August 14, 2018. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf
12. California Privacy Protection Agency. (2024). California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act.
13. https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf
14. Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.
15. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
16. Council of Europe. (1981). Convention for the protection of individuals with regard to automatic processing of personal data. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108
17. Council of Europe. (2018). Convention 108+: Convention for the protection of individuals with regard to the processing of personal data. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
18. European Data Protection Board. (2020a). Guidelines 05/2020 on consent under Regulation 2016/679. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
19. European Data Protection Board. (2020b). Guidelines 4/2019 on Article 25: Data protection by design and by default.
20. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
21. European Data Protection Supervisor. (2015). Towards a new digital ethics: Data, dignity and technology.
22. https://www.edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf
23. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679: General Data Protection Regulation. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
24. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence: Artificial Intelligence Act. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
25. Floridi, L. (2019). Translating principles into practices of digital ethics: Five risks of being unethical. Philosophy & Technology, 32, 185–193. https://doi.org/10.1007/s13347-019-00354-x
26. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28, 689–707. https://doi.org/10.1007/s11023-018-9482-5

27. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation." AI Magazine, 38(3), 50–57.
28. https://doi.org/10.1609/aimag.v38i3.2741
29. Government of India. (2023). The Digital Personal Data Protection Act, 2023. India Code.
30. https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf
31. Great Britain. (2018). Data Protection Act 2018. The National Archives.
32. https://www.legislation.gov.uk/ukpga/2018/12/contents
33. Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws and many bills. Privacy Laws & Business International Report, 157, 14–18. https://doi.org/10.2139/ssrn.3381593
34. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, 169, 3–5.
35. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348
36. Information Commissioner's Office. (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
37. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399. https://doi.org/10.1038/s42256-019-0088-2
38. Kuner, C. (2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. European Law Blog. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/
39. Lynskey, O. (2014). Deconstructing data protection: The "added-value" of a right to data protection in the EU legal order. International and Comparative Law Quarterly, 63(3), 569–597. https://doi.org/10.1017/S0020589314000244
40. Mantelero, A. (2018). Artificial intelligence and data protection: Challenges and possible remedies. Council of Europe. https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6
41. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.
42. https://doi.org/10.1177/2053951716679679
43. Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/
44. Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
45. Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
46. People's Republic of China. (2021). Personal Information Protection Law of the People's Republic of China. National People's Congress.
47. https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
48. Richards, N. M., & King, J. H. (2014). Big data ethics. Wake Forest Law Review, 49, 393–432.
49. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2384174
50. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560. https://doi.org/10.2307/40041279
51. South African Government. (2013). Protection of Personal Information Act 4 of 2013.
52. https://www.gov.za/documents/protection-personal-information-act
53. Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239–273.
54. https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/
55. UNESCO. (2021). Recommendation on the ethics of artificial intelligence.
56. https://unesdoc.unesco.org/ark:/48223/pf0000381137
57. United Nations General Assembly. (1948). Universal Declaration of Human Rights.
58. https://www.un.org/en/about-us/universal-declaration-of-human-rights
59. United Nations Human Rights Council. (2021). The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights.
60. https://www.ohchr.org/en/documents/thematic-reports/ahrc4828-right-privacy-digital-age-report-united-nations-high
61. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data

Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

62. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160
63. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30, 75–89. https://doi.org/10.1057/jit.2015.5