DATA OWNERSHIP IN THE DIGITAL AGE: LEGAL PERSPECTIVES ON PERSONAL DATA AS PROPERTY

Md. Kamruzzaman Jahad

Early-Career Legal Researcher, Undergraduate Student of Law, Feni University

Email: kzjahad@feniuniversity.ac.bd

Abstract:

Data is the codified representation of information. Additionally, every past, present, and future step in the digital world is data. In ancient times, the economy was based on the exchange of gold. At one point, oil replaced gold and became the "liquid gold." Now, data is the new oil. Like oil, data-driven economics is growing exponentially with limited alternatives. However, this transformation has raised significant concerns regarding personal data ownership, control, and regulation, with individuals increasingly treated as products rather than rights-bearing entities.

This shift has sparked critical questions about the ownership and regulation of personal data. As data becomes a valuable asset, debates arise over whether it should be classified as property under legal frameworks. This paper explores the implications of classifying personal data as property, analyzing the potential benefits, challenges, and alternative models. By examining legal theories, existing regulations, and comparative jurisdictional approaches between South Asia and First-World countries, the paper provides a comprehensive analysis of the feasibility and desirability of recognizing personal data as property. It concludes with recommendations for balanced legal reforms that safeguard individual rights while promoting innovation in the digital economy.

Introduction:

By 2030, the global data economy is projected to reach $13 trillion, representing over 10% of global GDP,[1] yet individuals have little to no control over their personal data.

[1] Ben Jorgesen, 'Unlocking the Trillion-Dollar Digital Transparency Economy' (Medium, Mar 17, 2025) https://benjorgensen.medium.com/unlocking-the-trillion-dollar-digital-transparency-economy-5b5effd30e9f

If our personal data fuels the digital economy, should we not have ownership rights over it?

Rather, advocates argue that granting individuals ownership rights over their data would empower them to negotiate with corporations, ensuring a fairer distribution of the economic value generated from their information.[2] This could address the imbalance in the current system, where companies profit disproportionately from data collection and processing.

While economic and ethical debates continue, the legal framework around data ownership remains underdeveloped and inconsistent, particularly in how different jurisdictions conceptualize personal data under property law.

The Facebook-Cambridge Analytica scandal,[3] which came to light in March 2018, exposed significant ethical and legal concerns regarding data privacy and ownership. Cambridge Analytica,[3] a political consulting firm, harvested personal data from over 87 million Facebook users through the app "This Is Your Digital Life," developed by Aleksandr Kogan.[4] While users of the app consented to data collection, their friends' data was accessed without consent, highlighting a major flaw in Facebook's policies.

Data has increasingly been compared to oil as a key economic resource due to its transformative role in the digital economy. Also, it is compared to infrastructure and an asset.[5] This analogy highlights its immense value when refined, its capacity to drive innovation, and its influence on global power dynamics. Yet, unlike oil or other

---

[2] Mira Burri, 'Big Data and Global Trade Law' in Florent Thouvenin and Aurelia Tamò-Larrieux (eds), (Cambridge University Press, 2021)

[3] Christophe Olivier Schneble, Bernice Simone Elger, and David Shaw, 'The Cambridge Analytica affair and Internet‐mediated research' (2018) EMBO rep https://www.embopress.org/doi/full/10.15252/embr.201846579

[4] Facebook–Cambridge Analytica data scandal, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[5] Jan Nolin, 'Data as Oil, Infrastructure, or Asset? Three metaphors of data as economic value' (Semantic Scholar, 2019) https://www.semanticscholar.org/paper/Data-as-oil%2C-infrastructure-or-asset-Three-of-data-Nolin/acbcadc9d97f847c9db6a5a4299869ea6cb360c6

tangible assets, data is intangible, easily replicated, and deeply personal, raising complex questions about its legal status.

This has led to a fundamental debate: Should personal data be treated as property, granting individuals ownership and the right to monetize it? Or does commodifying personal information risk undermining privacy and human dignity? Legal systems worldwide remain divided, with frameworks like the EU's GDPR[6] emphasizing privacy rights rather than ownership and other jurisdictions offering only piecemeal protections.

This paper explores the viability and consequences of recognizing personal data as property through a comparative legal analysis of South Asian and First-World jurisdictions, aiming to propose balanced reforms for digital governance.

Theoretical and Conceptual Background:

Understanding the legal and philosophical foundations of personal data ownership is essential to navigating the complex debates surrounding data rights in the digital age. This section anchors the discussion in classical property law theories, human rights principles, and evolving regulatory frameworks, offering a critical lens through which to assess both the legitimacy and the limitations of treating personal data as a form of property.

By engaging with foundational concepts such as the Lockean labor theory and Hohfeldian rights analysis, alongside modern frameworks of personal autonomy and informational self-determination, this analysis elucidates the normative justifications for recognizing individual claims to data ownership. At the same time, it interrogates the practical challenges such recognition entails, particularly in a landscape shaped by asymmetrical power relations between individuals and data-driven corporations.

Furthermore, the discussion draws on comparative insights from jurisdictions such as the European Union, the United States, India, Bangladesh, and Pakistan. By contrasting robust regimes like the EU's GDPR with the legislative gaps in South

[6] General Data Protection Regulation, GDPR [2016] OJ L 119

Asia, particularly in Bangladesh and Pakistan, it highlights the urgent need for nuanced, context-sensitive models of data governance. This theoretical groundwork serves as a foundation for the subsequent legal analysis and policy evaluation and sets the stage for proposing a reimagined framework for digital rights in the era of data capitalism.

The Lockean Labor Theory holds that property rights arise when an individual mixes their labor with unowned resources, thereby creating value and a moral claim to ownership.[7] Applied to data, this theory suggests that because individuals generate data through their actions, choices, and online behaviors,[8] they have a legitimate claim to ownership of the data they produce.[9]

Philosophers and legal theorists have extended this argument to personal data, contending that users are the "original owners" of their personhood, bodies, and minds, and thus also of the information that constitutes their personal identity.[10] When individuals interact online-posting content, making purchases, or sharing preferences, they effectively "mix their labor" with digital platforms, producing data that did not previously exist.[11] And as these data translate directly into monetizable datasets. If labor creates value, then individual autonomy and selfhood embedded in data arguably justify partial proprietary claims.

Wesley Hohfeld's analytical framework breaks down legal rights into four primary categories: claims, liberties, powers, and immunities, each with corresponding duties,

---

[7] John Locke's 'Labor theory of Property' https://en.wikipedia.org/wiki/Labor_theory_of_property

[8] Jakob Thrane Mainz (2021) But anyone can mix their labor: a reply to Cheneval, Critical Review of International Social and Political Philosophy, 24:2, 276-285, https://www.tandfonline.com/doi/full/10.1080/13698230.2020.1764786

[9] Craig Lambert, 'A Lockean case for the ownership of personal data' (2016) Mark Carrigan, https://markcarrigan.net/2016/04/29/a-lockean-case-for-the-ownership-of-personal-data/

[10] Jakob Thrane Mainz (2021) But anyone can mix their labor: a reply to Cheneval, Critical Review of International Social and Political Philosophy, 24:2, 276-285, https://www.tandfonline.com/doi/full/10.1080/13698230.2020.1764786

[11] Nathan Pelgrims, 'Work without author: Lockean theories of intellectual property and the product of artificial intelligence' (2020-2021) Faculteit Letteren en Wijsbegeerte https://libstore.ugent.be/fulltxt/RUG01/003/007/447/RUG01-003007447_2021_0001_AC.pdf

no-rights, liabilities, and disabilities. Applying this framework to data rights clarifies the fragmented and often incomplete legal entitlements individuals currently hold over their personal data.

Let's say, for example, the definition of claim rights is an entitlement to require another party to act or refrain from acting in a certain way, with a corresponding duty on that party.[12] Under data protection regimes like the GDPR, individuals have claim rights to access, rectify, or erase their personal data.[13] Data controllers (e.g., companies) have corresponding duties to comply with these requests. So the limitation is that these claim rights are often limited in scope and may not extend to all uses or transfers of data.

Beyond property, the concept of personal autonomy is central to normative claims over data. Informational self-determination, a principle rooted in German constitutional jurisprudence, emphasizes the individual rights to control the disclosure and use of their personal data.[14] This is more than a privacy guarantee, it is an assertion of personal agency.

However, Guggenberger argues that informational private autonomy as the basis for data control is unrealistic and potentially counterproductive in the data economy.[15] Gstrein proposes "data autonomy" as a framework expanding beyond individual rights to include organizational autonomy and address AI-related risks.[16] In Brazil, the General Data Protection Law reinforces private autonomy by requiring consent for

---

[12] Hohfeld's Concepts of Rights, UOLLB First Class Law Notes, (2024) https://uollb.com/blogs/uol/hohfeld-s-concepts-of-rights

[13] General Data Protection Regulation, GDPR [2016] OJ L 119

[14] Henne, T., & Gstrein, O. J. (2023). Governing the 'datafied' school: Bridging the divergence between universal education and student autonomy. In A. Zwitter, & O. Gstrein (Eds.), Handbook on the Politics and Governance of Big Data and Artificial Intelligence (pp. 395-428). (Political Science and Public Policy). Edward Elgar. https://doi.org/10.4337/9781800887374.00025

[15] Leonid Guggenberger, 'Irrweg informationelle Privatautonomie' (2023), https://doi.org/10.5771/9783748918196

[16] Gstrein, Oskar Josef, Data Autonomy: Recalibrating Strategic Autonomy and Digital Sovereignty (May 10, 2023). SSRN: http://dx.doi.org/10.2139/ssrn.4444191

personal data use.[17] The concept of data autonomy is particularly relevant in educational settings, where the datafication of schools raises concerns about student privacy and autonomy.[18] These perspectives highlight the ongoing debate surrounding personal autonomy in data governance and its practical implications.

The European Union's General Data Protection Regulation (GDPR) emphasizes individual rights, including the "right to be forgotten," and imposes significant fines for non-compliance.[19] In contrast, the United States lacks comprehensive federal legislation, relying on sector-specific laws like the California Consumer Privacy Act (CCPA), which focuses on specific industries or data types.[20] Both frameworks incorporate principles of transparency, consent, and data breach notification.[21] The GDPR and CCPA differ in their approach to privacy rights, with implications for future legislation.[22] India's Digital Personal Data Protection Act (DPDPA) of 2023 is benchmarked against global counterparts, identifying ambiguities and suggesting reforms based on best practices from the EU, Singapore, the USA, and Australia.[23]

---

[17] Lucas Gonçalves da Silva, Bricio Luis da Anunciação Melo, 'A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA AUTONOMIA PRIVADA EM UM MUNDO CADA VEZ MAIS TECNOLÓGICO' (2023), Revista Jurídica, https://doi.org/10.21902/revistajur.2316-753x.v3i56.3581

[18] Henne, T., & Gstrein, O. J. (2023). Governing the 'datafied' school: Bridging the divergence between universal education and student autonomy. In A. Zwitter, & O. Gstrein (Eds.), Handbook on the Politics and Governance of Big Data and Artificial Intelligence (pp. 395-428). (Political Science and Public Policy). Edward Elgar. https://doi.org/10.4337/9781800887374.00025

[19] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, Nkechi Emmanuella Eneh, 'DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS' (2024) Computer Science & IT Research Journal , 5(3), 528-543. https://doi.org/10.51594/csitrj.v5i3.859

[20] MarcusAbreu de Magalhaes, 'Data protection regulation: a comparative law approach' (2021) International Journal of Digital Law https://doi.org/10.47975/ijdl.magalhaes.v.2.n.2

[21] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, Nkechi Emmanuella Eneh, 'DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS' (2024) Computer Science & IT Research Journal https://doi.org/10.51594/csitrj.v5i3.859

[22] Srikrishna Deva Rao, 'The Evolution of Privacy Rights in the Digital Age: A Comparative Analysis of GDPR and CCPA' (2024) Indian Journal of Law https://doi.org/10.36676/ijl.v2.i4.40

[23] Mathew Chacko and Shambhavi Mishra, 'Benchmarking the Indian Digital Personal Data Protection Act 2023 against data protection frameworks in Singapore, the EU, US and Australia' (2023) Journal of Data Protection & Privacy, 6 (2), 110-119 https://doi.org/10.69554/LXHZ9342

These diverse regulatory landscapes necessitate a nuanced approach to global data privacy compliance.[24]

Bangladesh currently lacks comprehensive data protection legislation, despite growing privacy concerns in the digital age.[25] While privacy is conditionally recognized in the Constitution and some subsidiary laws, the existing legal framework is inadequate compared to international standards.[26] The absence of omnibus data privacy legislation is identified as a major challenge in protecting citizens' privacy rights.[27] In response, the government released the Data Protection Act, 2022 for public comment in April 2022.[28] This bill, although not yet enacted, includes provisions for extra-territorial application, consent-based processing, and the establishment of a Data Protection Office.[29] However, the proposed legislation has limitations, such as the exclusion of pseudonymous data and a non-independent regulator.[30] Enacting comprehensive data protection legislation is crucial for establishing an effective privacy protection regime in Bangladesh.[31]

Pakistan's legal landscape regarding data protection is evolving, but challenges remain. While the country has existing cybercrime laws, such as the Prevention of Electronic Crimes Act (PECA) 2016, their enforcement and management are

---

[24] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, Nkechi Emmanuella Eneh, 'DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS' (2024) Computer Science & IT Research Journal , 5(3), 528-543. https://doi.org/10.51594/csitrj.v5i3.859

[25] Md. Toriqul Islam, 'ADEQUACY OF PRIVACY REGIME IN BANGLADESH: KEY CHALLENGES AND POTENTIAL POLICY MEASURES' (2022) IIUM Law Journal https://doi.org/10.31436/iiumlj.v30i1.655

[26] Ibid

[27] Ibid

[28] G. Greenleaf, 'Bangladesh's Data Protection Bill' (2023) Social Science Research Network https://doi.org/10.2139/ssrn.4343782

[29] Ibid

[30] Ibid

[31] Md. Toriqul Islam, 'ADEQUACY OF PRIVACY REGIME IN BANGLADESH: KEY CHALLENGES AND POTENTIAL POLICY MEASURES' (2022) IIUM Law Journal https://doi.org/10.31436/iiumlj.v30i1.655

inadequate.[32] Recent research proposes a model law to enhance data protection and critical infrastructure security, addressing current shortcomings.[33] Comparative studies with India reveal the need for comprehensive reforms in Pakistan's proposed Personal Data Protection Bill, 2023.[34] Despite Islamic principles emphasizing privacy rights, as reflected in the Quran and Pakistani Constitution, the primary motivation for data protection legislation appears to be compliance with EU regulations to facilitate data flow and outsourcing opportunities.[35] These studies collectively highlight the necessity for Pakistan to develop and implement robust data protection laws that balance international standards with local cultural and religious contexts.

Current approaches to data protection often prioritize either corporate interests or public security, neglecting individual ownership. The debate around "data as property" raises questions about legal innovation versus dangerous commodification of identity.[36] While a property rights model for personal data has some appeal, it may not adequately address modern data protection challenges, particularly in context-aware computing.[37] Some argue for a holistic approach to data regulation, balancing stakeholder interests and treating industrial and user-generated data as distinct categories.[38] Others propose alternatives like the information fiduciary model to

---

[32] Rashid Zahoor, Naseem Razi, 'Analyzing the Cyberspace Laws to Protect Data Privacy in Pakistan' (2021), Law, State and Telecommunications Review https://doi.org/10.26512/lstr.v13i2.35977

[33] Muhammad Jawad Hadi, 'Safeguarding Critical Infrastructures Through Data Protection Laws: A Comparative Study with a Focus on Pakistan' (2024), Social Science Research Network, https://doi.org/10.2139/ssrn.4730720

[34] Muhammad Imran Ali and Khadeeja Ahmad Hussain, 'Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan' (2024), Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law, https://doi.org/10.25143/socr.28.2024.1.01-08

[35] Muhammad Hayat, 'Privacy and Islam: From the Quran to data protection in Pakistan' (2007), Law, Political Science - Information & Communications Technology Law. https://doi.org/10.1080/13600830701532043

[36] C. Prins, 'Property and Privacy: European Perspectives and the Commodification of Our Identity' (2006) Semantic Scholar, https://www.semanticscholar.org/paper/Property-and-Privacy%3A-European-Perspectives-and-the-Prins/72b28539a6aa076ff289b131b160525156acb32b

[37] Ibid

[38] Sanjit Kumar Chakraborty, Alex K. Koshy, Anjana Raghunath, 'Data As Property: Towards a Property Based Model?' (2023) Global Privacy Law Review Volume 4, Issue 4 pp. 181–193. https://doi.org/10.54648/gplr2023025

protect privacy and restructure the information economy.[39] The concept of data propertization becomes more complex in the context of big data and the quantified self movement, with some arguing that raw data, when part of a dataset, can be considered property.[40] These perspectives highlight the ongoing debate about data ownership and protection in the digital age.

Legal, ethical, and philosophical debates converge in the realization that a one-size-fits-all approach to data governance is untenable. A hybrid framework—incorporating proprietary rights, regulatory safeguards, and fiduciary duties—may offer a balanced path forward. Such a model should distinguish between user-generated and industrial data, enforce contextual consent, and establish clear lines of accountability in AI-driven systems.

This theoretical scaffolding—rooted in classical jurisprudence but responsive to contemporary digital realities—lays the foundation for reimagining data rights in a way that affirms both individual dignity and democratic oversight in the information age.

Methodology and Findings:

1. **Research Design and Jurisdictional Justification:**

This paper employs a comparative legal analysis to examine how different jurisdictions conceptualize, regulate, and enforce rights over personal data, with a particular focus on the idea of data as property. The comparative approach allows for a nuanced understanding of the evolving legal landscape across five key jurisdictions: the European Union (EU), the United States (US), India, Bangladesh, and Pakistan. These jurisdictions were selected for their diverse legal traditions, levels of digital infrastructure, and regulatory maturity. By juxtaposing established frameworks (such

[39] Talia Bank, 'Putting the Price on Privacy: Decommodifying Data with the Fiduciary Model' (2023) Macalester Street Journal https://doi.org/10.62543/msj.v1i1.10

[40] Argyro P. Karanasiou, Emile Douilhet, 'Never Mind the Data: The Legal Quest over Control of Information & the Networked Self' (2016) 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW) https://doi.org/10.1109/IC2EW.2016.39

as the GDPR in the EU) with emerging or fragmented regimes (such as in South Asia), this method aims to identify convergences, divergences, and potential avenues for legal development in the Global South.

By systematically comparing statutory frameworks, regulatory mechanisms, and jurisprudential interpretations, the research seeks to evaluate both the normative coherence and the practical enforceability of data ownership claims. This approach is particularly apt given the transnational nature of data flows and the persistent fragmentation of legal responses across jurisdictions.

The concept of data ownership and digital asset regulation presents complex challenges in the modern legal landscape. Comparative analyses reveal diverse approaches across jurisdictions in conceptualizing and regulating data ownership and protection.[41] While traditional property laws struggle to accommodate intangible digital assets, there's a growing recognition of the need for new legal frameworks.[42] Proposed solutions include applying intellectual property theories to big data,[43] establishing proprietary rights over digital artifacts,[44] and developing context-specific data rights.[45] Technological tools like blockchain and homomorphic encryption are being explored to facilitate data rights management.[46] The challenge lies in balancing commercial interests with public welfare, necessitating international agreements and

[41] Sardor Mamanazarov, 'Intellectual Property Theories as Applied to Big Data' (2024), International journal of law and policy, https://doi.org/10.59022/ijlp.164

[42] Andrea Boerding, Nicolai Culik, C. Doepke, T. Hoeren, Tim Juelicher, Charlotte Roettgen, Max V. Schoenfeld, 'Data Ownership—A Property Rights Approach from a European Perspective' (2018), Journal of Civil Law Studies, https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1221&context=jcls

[43] Sardor Mamanazarov, 'Intellectual Property Theories as Applied to Big Data' (2024), International journal of law and policy, https://doi.org/10.59022/ijlp.164

[44] Sardor Mamanazarov, 'DATA OWNERSHIP RIGHTS: FEASIBLE? LEGAL AND TECHNICAL SOLUTIONS' (2023), Tsul legal report, https://doi.org/10.51788/tsul.lr.4.4./gvtj6320

[45] Sardor Mamanazarov, 'Intellectual Property Theories as Applied to Big Data' (2024), International journal of law and policy, https://doi.org/10.59022/ijlp.164

[46] Sardor Mamanazarov, 'DATA OWNERSHIP RIGHTS: FEASIBLE? LEGAL AND TECHNICAL SOLUTIONS' (2023), Tsul legal report, https://doi.org/10.51788/tsul.lr.4.4./gvtj6320

multi-stakeholder collaboration.[47] As digital assets become increasingly integrated into global economies, a harmonized approach to regulation is crucial.[48]

Comparative legal research in this context allows for a nuanced understanding of the divergent models: for example, the United States, through the CCPA, tends to treat personal data as a tradable asset, enabling monetization with limited consumer rights, while the European Union's GDPR frames personal data as an inalienable right, prioritizing individual control and privacy over commodification. Other jurisdictions, such as Indonesia, adopt hybrid approaches that combine fundamental rights with regulated cross-border data transfers. This methodological design enables the identification of key challenges-such as regulatory fragmentation, compliance complexity, and disparities in consumer protection-and highlights the need for greater harmonization and international cooperation in data governance.

By focusing on both doctrinal analysis and evaluative comparison, this research design provides a robust foundation for assessing whether traditional property concepts are adequate for personal data or whether new legal paradigms are necessary to address the unique characteristics of data in the digital age.

2. Jurisdictional Overview and Core Doctrinal Sources:

The European Union's General Data Protection Regulation (GDPR) serves as the global gold standard for privacy-centric regulation, emphasizing fundamental rights (e.g., access, erasure) and strict corporate accountability. Its extraterritorial reach and principles of transparency and consent provide a baseline for evaluating other frameworks. Primarily, the EU's GDPR serves as a benchmark in this regard.[49]

[47] Luke Lee, 'Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches' (2024), Social Science Research Network, https://doi.org/10.2139/ssrn.4807135

[48] Ibid

[49] Ruben de Bruin, 'A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence' (2022), Social Science Research Network, https://doi.org/10.2139/ssrn.4251540

In contrast, the US adopts a market-centered approach, viewing individuals as "privacy consumers".[50] The California Consumer Privacy Act (CCPA) typifies the US's sectoral, decentralized approach, prioritizing consumer choice (e.g., opt-out rights) over comprehensive ownership. Unlike the GDPR, it avoids treating data as an inalienable right, reflecting a capitalist ethos where data is a tradable asset.

India's evolving framework, including the Digital Personal Data Protection Act (DPDPA) 2023, attempts to localize global norms while recognizing privacy as a fundamental right.[51] The DPDPA blends GDPR-inspired principles (consent, grievance redressal) with local adaptations, such as broad government exemptions and a focus on digital data.[52] However, gaps persist-e.g., no distinction between sensitive and ordinary data, omission of pseudonymization.

Bangladesh's Draft Data Protection Act offers insight into the normative and institutional challenges faced by developing legal systems.[53] Despite progressive provisions like consent-based processing and the establishment of a Data Protection Office, the draft law suffers from critical limitations, such as the exclusion of pseudonymous data from its scope and the absence of an independent regulatory authority. These shortcomings underscore the country's reliance on outdated legislation that prioritizes state security over individual privacy.

Finally, though Pakistan's data protection framework is underdeveloped, its constitutional recognition of privacy (via judicial interpretation) and ongoing legislative efforts offer insights into South Asia's struggle to reconcile traditional

---

[50] Ibid

[51] Nandinee Singh, 'Data Protection and Privacy as a Fundamental Right - An In-depth Analysis of the European Union and India's Data Protection Legislation' (2024), International Journal For Multidisciplinary Research, https://doi.org/10.36948/ijfmr.2024.v06i02.15869

[52] Sneha Mahawar, 'Major data protection statutes in the world: a comparative analysis' (2023), https://blog.ipleaders.in/major-data-protection-statutes-in-the-world-a-comparative-analysis/

[53] Wasif Jamal Khan, 'Bangladesh's proposed data protection framework in light of global standards' (2023), The Business Standard, https://www.tbsnews.net/thoughts/bangladeshs-proposed-data-protection-framework-light-global-standards-571482

norms with digital governance.[54] Pakistan's proposed Personal Data Protection Bill 2023 aims to enhance data protection measures.[55]

Collectively, these jurisdictions capture a broad range of legal traditions-from civil law in the EU to common law in the US and India, as well as hybrid systems in Bangladesh and Pakistan-and reflect varying policy priorities, from rights-based to market-driven and state-centric approaches. This selection enables the identification of systemic patterns, normative tensions, and opportunities for reform within the global data governance landscape.

3. Case Study Integration and Real-World Legal Controversies:

This study's primary data set comprises foundational legal texts, including statutes, draft bills, and regulatory guidelines from the jurisdictions under examination. These core materials provide the doctrinal basis for understanding how personal data ownership and protection are legally framed and enforced. Complementing these are judicial decisions and rulings from data protection authorities, which offer critical insights into the practical application, interpretation, and evolution of data rights in real-world contexts. To ground the analysis in lived legal controversies and illustrate the tangible implications of regulatory frameworks, the research also incorporates landmark cases and incidents.

The Facebook-Cambridge Analytica scandal, which came to light in 2018, involved the unauthorized collection and exploitation of personal data from 87 million Facebook users for political purposes.[56] This incident highlighted significant ethical breaches by Facebook, including violations of its own code of conduct and data

---

[54] Muhammad Zain Alam and Ghaneem Irfan Warraich, 'A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORK FOR DATA PROTECTION IN GLOBAL JURISDICTIONS' (2024) Pakistan Journal of International Affairs, https://pjia.com.pk/index.php/pjia/article/download/1124/762/1255

[55] Muhammad Imran Ali and Khadeeja Ahmad Hussain, 'Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan' (2024), Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law, https://doi.org/10.25143/socr.28.2024.1.01-08

[56] Umut Özdemir, 'EXAMINATION OF THE FACEBOOK-CAMBRIDGE ANALYTICA SCANDAL IN THE FRAMEWORK OF PARTICIPATORY CULTURE, DIGITAL LABOR EXPLOITATION AND INVASION OF PRIVACY' (2022), Ege Üniversitesi İletişim Fakültesi Medya ve İletişim Araştırmaları Hakemli E-Dergisi, https://doi.org/10.56075/egemiadergisi.999935

policies.[57] The scandal exposed issues of digital labor exploitation, invasion of privacy, and the weaponization of consumer data.[58] Cambridge Analytica used the collected data to create detailed behavioral profiles, which were then employed to influence voting behavior in the 2016 US presidential election.[59] The incident sparked global discussions on data protection, potential regulations for tech giants, and the need for greater transparency in data collection practices.[60] It also raised questions about Facebook's responsibility in safeguarding user privacy while maintaining its advertising-based revenue model.[61]

The Aadhaar project, India's biometric identification system, has been the subject of significant litigation and debate. While proponents argue it facilitates government welfare programs and improves service delivery,[62] critics raise concerns about privacy, data security, and constitutional rights.[63] The implementation of Aadhaar has faced legal challenges, including the landmark case of Justice K. S. Puttaswamy v. Union of India, which addressed the constitutionality of the scheme.[64] Despite the Supreme Court upholding citizens' right to privacy, the government continues to push for widespread adoption of Aadhaar.[65] The program's evolution from voluntary to

---

[57] Nikhil Arora, Darius Zinolabedini, 'The Ethical Implications of the 2018 Facebook-Cambridge Analytica Data Scandal' (2019), Texas ScholarWorks, University of Texas Libraries, https://doi.org/10.26153/TSW/7590

[58] M. Bofa, Darmawan Wawan Budi, Arifin Sudirman, 'Data Rights di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook dalam Pemilihan Presiden Amerika Serikat 2016' (2022), Hasanuddin Journal of International Affairs, https://doi.org/10.31947/hjirs.v2i2.22686

[59] Ibid

[60] Tami Kim, Gerry Yemen, 'Facebook, Cambridge Analytica, and the (Uncertain) Future of Online Privacy' (2020), Social Science Research Network, https://doi.org/10.2139/ssrn.3660467

[61] Ibid

[62] R. Krishna, 'Data Management in India: A Case Study of Aadhaar Project' (2020), Emerald Publishing Limited, https://doi.org/10.1108/978-1-80043-884-220211008

[63] N. V. Mali, Martha A. Avila-Maravilla, 'Convergence or Conflict?: Digital Identities vs. Citizenship Rights: Case Study of Unique Identification Number, Aadhaar, in India' (2018), International Conference on Theory and Practice of Electronic Governance, https://doi.org/10.1145/3209415.3209487

[64] R. Krishna, 'Data Management in India: A Case Study of Aadhaar Project' (2020), Emerald Publishing Limited, https://doi.org/10.1108/978-1-80043-884-220211008

[65] T. Satpathy, 'The Aadhaar: "Evil" Embodied as Law' (2017), Health technology, https://doi.org/10.1007/s12553-017-0203-5

mandatory has sparked criticism and legal disputes.[66] The Aadhaar litigation highlights the tension between technological innovation in governance and the protection of individual rights, serving as a potential precedent for similar debates globally.[67]

In a significant data privacy breach case in Bangladesh, a lawsuit has been filed against Sajeeb Wazed Joy, former ICT adviser and son of former Prime Minister Sheikh Hasina, along with former State Minister for ICT Zunaid Ahmed Palak and 17 others, accusing them of conspiring to sell sensitive National Identification (NID) data of over 110 million Bangladeshi citizens.[68] The case, lodged under the Cyber Security Act at Kafrul Police Station by complainant Enamul Haque, alleges that Joy and Palak abused their official positions to facilitate the unauthorized sale of personal information through an organized syndicate.

According to the case statement, the defendants allowed Digicon Global Services Limited to access and commercially exploit the NID database without adequate safeguards for national security or data privacy. The data was reportedly sold to approximately 182 domestic and international entities, raising serious public security concerns. The syndicate is also accused of embezzling around Tk 20,000 crore (approximately $1.8 billion) from these transactions.[69]

A company named Digicon Global Services Limited was allegedly permitted to use the NID data for business dealings without ensuring national security and personal

---

[66] Oshank Sharma, 'Right to Privacy and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.' (2020), Law, Political Science, https://www.semanticscholar.org/paper/Right-to-Privacy-and-the-Aadhaar

[67] N. V. Mali, Martha A. Avila-Maravilla, 'Convergence or Conflict?: Digital Identities vs. Citizenship Rights: Case Study of Unique Identification Number, Aadhaar, in India' (2018), International Conference on Theory and Practice of Electronic Governance, https://doi.org/10.1145/3209415.3209487

[68] 'Joy, Palak sued for selling NID information' (2024), The Daily Star, https://www.thedailystar.net/news/bangladesh/crime-justice/news/joy-palak-sued-selling-nid-information-3723621

[69] 'Ex-director of Data Centre arrested' (2024), Dhaka Tribune, https://www.dhakatribune.com/bangladesh/361389/ex-director-of-data-centre-arrested

data protection.[70] The case highlights significant concerns about data privacy and security in Bangladesh, where comprehensive data protection legislation is still developing.

A recent episode involving Mohammad Rony, a watermelon seller at Dhaka's Karwan Bazar,[71] vividly illustrates the legal and practical gaps in personal data and digital identity protection in Bangladesh. Rony's energetic and humorous sales chants-such as "Oi kiree, oi kiree"—turned him into a viral sensation across TikTok, YouTube, and other social media platforms, rapidly drawing thousands of visitors and content creators to his stall.

However, instead of reaping financial rewards, Rony faced overwhelming crowds more interested in filming than buying, leading to significant business losses-he reported unsold stock worth approximately 1.5 lakh BDT and mounting stress.[72] While companies and brands capitalized on his newfound fame for marketing and promotional content, many failed to deliver promised deals or compensation.[73] As Rony's personal brand-rooted in his unique personality and labor-became a digital asset widely shared and monetized by others, he retained no control or means to benefit from its exploitation.

Rony's experience underscores a critical gap: in the absence of comprehensive data protection or personality rights legislation, viral fame in Bangladesh can result in the widespread, unauthorized commercial use of an individual's identity, image, and

[70] Niva Yadav, 'Former data center director jailed in Bangladesh after selling personal information of 110 million people' (2024), Data Center Dynamics, https://www.datacenterdynamics.com/en/news/former-data-center-director-jailed-in-bangladesh-after-selling-personal-information-of-110-million-people/

[71] Ariful Hasan Shuvo, 'How going viral backfired for a watermelon seller in Karwan Bazar' (2025), The Business Standard, https://www.tbsnews.net/features/panorama/how-going-viral-backfired-watermelon-seller-karwan-bazar-1104966

[72] Business Inspection BD, https://www.linkedin.com/posts/businessinspectionbd_mohammad-rony-the-popular-watermelon-seller-activity-7307285163711897601-swKo/

[73] Ariful Hasan Shuvo, 'How going viral backfired for a watermelon seller in Karwan Bazar' (2025), The Business Standard, https://www.tbsnews.net/features/panorama/how-going-viral-backfired-watermelon-seller-karwan-bazar-1104966

creative expression, with little recourse or protection for the original creator. This case highlights the urgent need for legal reforms that recognize and safeguard the rights of individuals over their digital identity and personal brand in the age of social media virality.

The rise of digital platforms and social media has transformed the landscape of personal branding and content creation. While these platforms offer opportunities for individuals to gain visibility and potentially monetize their online presence,[74] they also present challenges in terms of control and economic benefit. Content creators often engage in continuous, cross-platform labor to maintain their online personae, despite uncertainty about financial outcomes.[75] The current copyright system may not adequately protect creators' interests in the social media age, where personal brand and attribution rights are increasingly important.[76] While digital platforms can provide benefits such as access to education and improved consumer experiences,[77] they also raise concerns about monopoly power, inequality, and labor exploitation.[78] The rapid growth of mobile internet and social networking has led to an unprecedented boom in viral content,[79] further complicating the dynamics of digital word-of-mouth and media quality.

Similarly, the recent viral trend of using AI to generate Ghibli-style artwork-inspired by Studio Ghibli's iconic animation style-has exposed critical gaps in data governance, ownership rights, and user control over personal information. Users are often required to upload personal images without transparent information regarding

---

[74] Leah M. Scolere, Urszula Pruchniewska, B. Duffy, 'Constructing the Platform-Specific Self-Brand: The Labor of Social Media Promotion' (2018) Social Media + Society, Sage Journals, https://doi.org/10.1177/2056305118784768

[75] Ibid

[76] Z. Blumenfeld, 'Selling the Artist, Not the Art: Using Personal Brand Concepts to Reform Copyright Law for the Social Media Age' (2018), Columbia Law School, https://doi.org/10.7916/JLA.V42I2.2007

[77] B. Nicholson, Petter Nielsen, Johan Saebo, 'Digital platforms for development' (2021), Information Systems Journal, https://doi.org/10.1111/isj.12364

[78] Ibid

[79] Gian Fulgoni and Andrew Lipsman, 'The Downside of Digital Word of Mouth And the Pursuit of Media Quality' (2017), Journal of Advertising Research, https://doi.org/10.2501/JAR-2017-020

data retention, usage, or deletion policies. Consequently, uploaded photos-including embedded metadata-may be stored indefinitely, repurposed for AI training, or commercialized without users' informed consent.

Each case is analyzed through a doctrinal lens, incorporating constitutional jurisprudence, legislative frameworks, regulatory actions, and public interest litigation. These legal sources are complemented by contextual analysis, recognizing the political economy and socio-technical architecture within which data ownership debates unfold.

4. Analytical Framework: Dimensions of Data Ownership:

To systematically evaluate the approaches to personal data governance across selected jurisdictions, this study employs a unified analytical framework centered on four key dimensions: (1) recognition of data as property; (2) scope of individual rights; (3) institutional enforcement mechanisms; and (4) the presence or absence of ownership-like control.

The first dimension, recognition of data as property, assesses whether and how each legal system conceptualizes personal data as a form of property, either explicitly through legislative language or implicitly through judicial interpretations. This includes analyzing the extent to which ownership rights, such as the rights to exclude, transfer, or derive income, are recognized or denied in relation to personal data.

The scope of individual rights, the second dimension, examines the breadth and depth of legal entitlements granted to individuals over their personal data. This encompasses rights to access, correct, delete, and port data, as well as the right to withdraw consent for processing. The analysis considers the extent to which these rights are effectively enforceable and whether they align with principles of autonomy and informational self-determination.

The third dimension, institutional enforcement mechanisms, evaluates the effectiveness, independence, and resources of regulatory bodies, judicial oversight, and complaint redressal systems responsible for upholding data protection laws. This

includes assessing the powers of data protection authorities, the availability of judicial remedies, and the accessibility of dispute resolution processes for individuals.

Finally, the fourth dimension, the presence or absence of ownership-like control, investigates the degree to which individuals can exercise control over their personal data akin to traditional property ownership. This includes the ability to transfer, license, or monetize data, as well as any legal or practical limitations that restrict such control.

A qualitative content analysis is applied to extract thematic consistencies and divergences from the legal texts and interpretive commentaries within each jurisdiction. This method facilitates a nuanced understanding of how each regime balances individual autonomy, corporate interests, and public policy considerations in the governance of personal data.

5. Methodological Constraints and Mitigation Strategies:

A qualitative content analysis is applied to extract thematic consistencies and divergences from the legal texts and interpretive commentaries within each jurisdiction. This method facilitates a nuanced understanding of how each regime balances individual autonomy, corporate interests, and public policy considerations in the governance of personal data.

While the chosen methodology offers a rigorous framework for comparative legal analysis, it is subject to several inherent limitations. First, data protection laws are dynamic and rapidly evolving, with frequent amendments, emerging case law, and shifting regulatory interpretations that may outpace the temporal scope of this study. Consequently, the analysis primarily reflects the legal landscape as it stands at the time of research, potentially limiting its applicability to future developments.

Second, the methodology centers on de jure legal provisions and formal regulatory frameworks, which may diverge from de facto practices on the ground. Enforcement gaps, institutional capacity constraints, and cultural factors can significantly influence

how data governance operates in practice, nuances that are not fully captured by doctrinal analysis alone.

Third, jurisdictional differences in legal terminology, enforcement cultures, and political economy present challenges for direct comparison. Variations in how concepts like “ownership,” “consent,” or “privacy” are defined and operationalized can complicate cross-jurisdictional synthesis.

To mitigate these limitations, the study anchors its analysis in broad, cross-jurisdictional principles of data governance and privacy rights while maintaining contextual sensitivity to local legal, social, and economic realities. This approach balances the need for comparative rigor with an appreciation of the complex, situated nature of data protection regimes worldwide.

Critical Discussion: Reimagining Data Ownership in the Digital Age:

This section critically analyzes the comparative findings presented earlier, reflecting on their implications for legal theory, policy reform, and data governance, particularly in emerging economies. Because, even if scrolling on the phone and thinking of something in mind, the built-in algorithm tracks it and shows the products, the economy is running. It argues that traditional property law frameworks are insufficient to address the unique challenges posed by personal data in the digital age. The discussion highlights the necessity of hybrid rights models that balance individual autonomy, corporate interests, and public oversight. By exploring these themes, this section aims to illuminate pathways for developing more equitable and effective data governance regimes that respond to both global standards and local realities. Ultimately, it underscores the urgency of legal innovation to protect data rights in an increasingly interconnected world.

1. Reconceptualizing Ownership:

This theme explores whether personal data should be treated as a form of property-alienable, tradable, and inheritable-or as an extension of personality rights, which are inalienable and rooted in human dignity.[80] The discussion will critically engage with the strengths and limitations of both models, considering arguments that property rights could empower individuals to negotiate with data controllers,[81] versus concerns that commodification risks eroding fundamental rights and personal autonomy.[82]

---

[80] Lusine Vardanyan, Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022), Journal of Ethics and Legal Technologies, 4(1), 105-120. 10.14658/pupj-JELT-2022-1-7 https://jelt.padovauniversitypress.it/2022/1/7

[81] Paulius Jurcys, Christopher Donewald, Mark Fenwick, Markus Lampinen, Vytautas Nekrošius, and Andrius Smaliukas, 'Ownership of User-Held Data: Why Property Law is the Right Approach' (2021), Harvard Journal of Law and Technology (JOLT), https://jolt.law.harvard.edu/assets/digestImages/Paulius-Jurcys-Feb-19-article-PJ.pdf

[82] Florent Thouvenin and Aurelia Tamò-Larrieux, 'Big Data and Global Trade Law' (2021), 15 - Data Ownership and Data Access Rights Meaningful Tools for Promoting the European Digital Single Market? from Part IV - Global Perspectives on Digital Trade Governance, Cambridge University Press, https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-ownership-and-data-access-rights/BC314C63C58A09C4B9C5D55894FE68C6

2. Power Asymmetry and Algorithmic Control:

This section examines the persistent imbalance of power between individuals and data controllers, particularly in the context of algorithmic decision-making and AI-driven data economies. It will highlight how current legal regimes often fail to address the realities of data extraction, profiling, and commercial exploitation, leaving individuals with limited practical control despite formal rights.[83] The analysis will draw on examples of data misuse and the challenges of enforcing meaningful consent and oversight in an era of pervasive surveillance and algorithmic opacity.

3. From Consent to Genuine Control: Rethinking Data Subject Autonomy:

Here, the focus shifts from traditional consent-based models to more robust forms of user control and informational self-determination.[84] The section will assess the effectiveness of existing data subject rights-such as access, rectification, erasure, and portability— and consider proposals for enhancing individual agency, including data portability, granular consent, and the right to object to or restrict processing.[85] The limitations of consent as a legal basis, especially in complex digital environments, will be critically evaluated.

4. Toward a Pluralist Legal Framework for Data in the Global South:

This final theme addresses the unique challenges and opportunities for data governance in emerging economies. It will analyze the normative gaps, institutional weaknesses, and socio-economic realities that shape data protection efforts in jurisdictions like Bangladesh, India, and Pakistan. The discussion will advocate for context-sensitive, pluralist legal frameworks that integrate global best practices with local needs, moving beyond one-size-fits-all solutions.

---

[83] IGS, 'Taking Data Ownership Seriously' (2023), Information Governance Services, https://www.informationgovernanceservices.com/articles/taking-data-ownership-seriously/

[84] Ibid

[85] Ibid

The foundational debate in the legal treatment of personal data centers on whether it should be regarded as a form of tradable property or as an intrinsic aspect of personality, protected by rights rooted in dignity and autonomy.[86] This conceptual distinction shapes not only the allocation and enforcement of rights, but also the broader logics governing digital economies and data-driven societies.[87]

In the United States, data governance is predominantly informed by a property-based logic, where personal data is treated as an economic asset that can be bought, sold, and licensed.[88] Proponents argue that recognizing data as property empowers individuals to control, monetize, and transfer their data, potentially rebalancing power in the digital marketplace.[89] However, critics contend that this commodification fragments identity and exposes individuals to new forms of exploitation, as the burden of negotiating complex data transactions falls disproportionately on users, who often lack bargaining power or technical literacy.[90] Moreover, treating data as property risks legitimizing surveillance capitalism, where personal identity is reduced to a set of monetizable data points.[91]

By contrast, European data law-most notably the General Data Protection Regulation (GDPR)—anchors personal data within the framework of personality rights,

---

[86] Henry Pearce, 'Personality, property and other provocations: exploring the conceptual muddle of data protection rights under EU law.' https://pure.port.ac.uk/ws/portalfiles/portal/13809188/Pearce_Personality_property_and_other_provocations.pdf

[87] Lusine Vardanyan and Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022), Journal of Ethics and Legal Technologies – Volume 4(1), https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-1-07.pdf

[88] Shivam Raj, 'Personal Data as Property: Unpacking Ownership, Rights, and Ethical Consideration' (2024), The Legal Quoram, https://thelegalquorum.com/personal-data-as-property-unpacking-ownership-rights-and-ethical-consideration/

[89] Ibid

[90] Worldbank, 'The debate over ownership of personal data', World Development Bank Report (2021), https://openknowledge.worldbank.org/server/api/core/bitstreams/fca03cbb-a6ad-53d8-b864-2a9e321afbe8/content

[91] Shivam Raj, 'Personal Data as Property: Unpacking Ownership, Rights, and Ethical Consideration' (2024), The Legal Quoram, https://thelegalquorum.com/personal-data-as-property-unpacking-ownership-rights-and-ethical-consideration/

emphasizing individual dignity, autonomy, and informational self-determination.[92] Here, rights such as erasure, rectification, and objection are not merely procedural; they reflect the view that personal data is inseparable from the person and thus fundamentally non-alienable.[93] The GDPR's approach is echoed in India's Justice K.S. Puttaswamy v. Union of India decision,[94] which constitutionalizes privacy as an extension of dignity and bodily integrity, rejecting a purely economic conception of data.

Yet, neither paradigm is wholly sufficient, especially in the context of the Global South, where legal systems must navigate the intersection of individual rights with collective, cultural, and developmental imperatives.[95] A rigid personality-based model may over-legalize data flows in resource-constrained environments, while a property-centric approach risks replicating historical patterns of resource extraction and inequality.[96]

Accordingly, a hybrid approach is increasingly advocated-one that combines the negotiability of property frameworks with the inalienability of personality-based protections.[97] Such a model would enable individuals to authorize limited uses of their data under clear fiduciary or contractual terms, while safeguarding core aspects of dignity through unwaivable rights, such as prohibitions on profiling or biometric misuse.[98] This hybrid vision is particularly salient for jurisdictions like Bangladesh

[92] Lusine Vardanyan and Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022), Journal of Ethics and Legal Technologies—Volume 4(1), https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-1-07.pdf

[93] Ibid

[94] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

[95] Lusine Vardanyan and Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022), Journal of Ethics and Legal Technologies—Volume 4(1), https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-1-07.pdf

[96] Worldbank, 'The debate over ownership of personal data', World Development Bank Report (2021), https://openknowledge.worldbank.org/server/api/core/bitstreams/fca03cbb-a6ad-53d8-b864-2a9e321afbe8/content

[97] Lusine Vardanyan and Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022), Journal of Ethics and Legal Technologies—Volume 4(1), https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-1-07.pdf

[98] Ibid

and Pakistan, where emerging data governance frameworks must address socio-economic inequality, low digital literacy, and centralized state power.

In sum, reconceptualizing data ownership as a synthesis of property and personality rights offers a pragmatic path forward, balancing individual agency, market innovation, and the protection of fundamental human interests in an increasingly data-driven world.[99]

Toward a Pluralist Legal Framework: Normative and Policy Innovations:

1. **Doctrinal Innovations:**

A pluralist approach to data governance in the Global South requires doctrinal innovations that move beyond imported models and respond to local realities. First, data should be recognized as a 'dual-aspect legal interest', encompassing both its economic value and its intrinsic connection to identity and dignity. This hybrid recognition enables negotiability, such as licensing for specific, limited uses-while prohibiting core violations, including unauthorized biometric profiling or exploitative algorithmic targeting.

Second, the introduction of 'data fiduciaries' is critical. Drawing on India's experience, imposing fiduciary duties of care, loyalty, and purpose limitation on data controllers reframes the relationship from a transactional exchange to one of trust. This is particularly important in contexts marked by low digital literacy and significant power asymmetries, where individuals are otherwise ill-equipped to negotiate fair terms.[100]

Third, certain personality-based rights must be 'unwaivable.' Rights such as protection from biometric surveillance, the right to be forgotten, and autonomy in profiling should be anchored in constitutional dignity principles and shielded from

---

[99] Ibid
[100] Charukeshi Bhatt and Anirudh Burman, 'Data Protection Regulation in the Global South' (2024), Carnegie Endowment for International Peace, https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south?lang=en

contractual waiver or state interference. This doctrinal safeguard ensures that the most fundamental aspects of personhood are not subject to commodification or coercion.[101]

Finally, the recognition of 'community data rights' is essential in postcolonial and collectivist contexts. Community ownership of data-especially in relation to indigenous knowledge, agricultural, or environmental resources-can counteract extractive data colonialism and empower marginalized groups. Community-centric governance models, informed by the knowledge commons framework, challenge the individualistic assumptions of globalized data policy and support more equitable outcomes.[102]

2. Policy and Regulatory Recommendations:

Effective implementation demands robust policy and regulatory measures. 'Independent Data Protection Authorities (DPAs)', with sufficient resources and autonomy, are vital for credible enforcement and public trust-moving beyond symbolic or politically influenced bodies.[103]

Mandatory 'algorithmic accountability mechanisms' -such as impact assessments, transparency audits, and public registers for high-risk AI systems-are necessary to address discrimination and opacity, particularly in sensitive sectors like health, welfare, and law enforcement.[104]

'Public legal education and digital literacy' initiatives must be institutionalized, ensuring that citizens are empowered to understand and assert their data rights. This is

---

[101] Cornelia Laras Gigih Kineta, Dr. Suci Lestari Yuana, 'Navigating the Net: India's Digital Governance as A Global South Vision in the Global Digital Order' (2024), Universitas Gadjah Mada, https://etd.repository.ugm.ac.id/penelitian/detail/242659

[102] Aditya Singh and Divij Joshi, 'The Histories, Practices, and Policies of Community Data Governance in the 'Global South'' (2023), Faculty of Laws University College London Law Research Paper No. 11/2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4506644

[103] Silvana Fumega, 'The Global Landscape of Data Governance' (2024), CIGI, https://www.cigionline.org/articles/the-global-landscape-of-data-governance/

[104] Charukeshi Bhatt and Anirudh Burman, 'Data Protection Regulation in the Global South' (2024), Carnegie Endowment for International Peace, https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south?lang=en

especially urgent in societies where awareness of privacy and data protection remains low.[105]

'Localized regulatory sandboxes' should be established to pilot innovative governance models, such as community consent protocols or decentralized data cooperatives, tailored to rural or under-resourced regions. These experimental frameworks enable context-sensitive solutions before scaling nationally.[106]

Finally, 'regional cooperation' is needed to harmonize cross-border data flows and resist digital dependency on dominant foreign actors. South Asian alliances can facilitate standard-setting, mutual capacity-building, and collective bargaining in the global digital economy.[107]

Integrative Insight:

These normative and policy innovations point toward a pluralist, dignity-respecting, and power-sensitive model of data governance for the Global South. Rather than replicating external templates, this approach reinterprets global standards through the lens of local realities, enabling redistributive justice, epistemic sovereignty, and genuine informational self-determination.

Conclusion:

The preceding analysis demonstrates that traditional property law frameworks, while illuminating, are fundamentally inadequate for addressing the complexities of personal data in the digital age-especially in the context of the Global South. Viewing data

[105] Ibid

[106] Sophie Tomlinson, 'Balancing data opportunities and challenges in the global south with innovative governance solutions' (2022), Datasphere Initiative, https://www.thedatasphere.org/news/balancing-data-opportunities-and-challenges-in-the-global-south-with-innovative-governance-solutions/

[107] Bitange Ndemo, 'Addressing digital colonialism: A path to equitable data governance' (2024), UNESCO Inclusive Policy Lab, https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance

solely through the lens of property risks commodifying individuals into extractable assets. Instead, a pluralist legal model-one that is rooted in human dignity, community, and individual autonomy-emerges as essential. Such a model recognizes the unique, relational, and often communal nature of data and insists on rights and responsibilities that transcend mere ownership.

At the heart of this inquiry are the divergent logics that underpin global data regulation: the property paradigm, which emphasizes individual control and monetization, and the personality paradigm, which foregrounds privacy, dignity, and self-determination. The real-world consequences of weak or fragmented data governance-ranging from exploitative surveillance to the disenfranchisement of marginalized communities-underscore the urgent need for reform. The promise of innovative legal constructs, such as fiduciary duties for data controllers, unwaivable data rights, and the recognition of community data sovereignty, offers a pathway toward more equitable digital futures.

While promising, the path to meaningful reform is fraught with complexity. Policymakers must prioritize institutional independence and algorithmic transparency, ensuring that regulatory bodies are empowered and insulated from undue influence. Regional legal harmonization-particularly within South Asia-can foster a more consistent and rights-respecting digital environment. Equally important is the cultivation of digital literacy and the active empowerment of marginalized groups so that all individuals can exercise agency over their data in practice, not just in theory. Implementation will require persistent vigilance against regulatory capture, as well as a commitment to adaptability in the face of evolving technological threats.

Ultimately, the struggle for data sovereignty is inseparable from the broader quest for justice and self-determination in the digital era. As data-driven systems increasingly mediate our identities, choices, and opportunities, the stakes of this debate become existential. In a world where algorithms know us better than we know ourselves, the legal right to self-determination must extend beyond flesh and into the digital mirror of our identities. The question is no longer whether we own our data, but whether we

own ourselves in the age of surveillance capitalism. The answer will define not just the contours of digital rights, but the very meaning of personhood in the twenty-first century.

Keywords: Data Ownership, Digital Sovereignty, Comparative Data Governance, Algorithmic Regulation, Digital Privacy Rights, Structural Transformation in Data Economies.