INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RESARCH PAPER ON GLOBALISATION IS A THREAT TO DATA PRIVACY

AUTHOR - NAINSI JAISWAL* & PROF. TAPAN CHANDOLA**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – NAINSI JAISWAL & PROF. TAPAN CHANDOLA, RESARCH PAPER ON GLOBALISATION IS A THREAT TO DATA PRIVACY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 660-671, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The structural threat of individual data privacy posed by globalization Due to the promotion of digital technology.and the movement of data across various national boundaries is one that requires strict academic consideration. This paper argues that the structural design of globalization systematically has undermined privacy protection in three intersecting processes. To begin with, the economic paradigm of surveillance capitalism that transnational businesses follow views personal information as a raw material that creates an imbalance of power, which essentially negates the informed user consent. Secondly, the fragmentation of national regulating systems promotes arbitrage of jurisdiction, in which actors take advantage of the differences in laws by using jurisdictions with less stringent protective laws, thus creating a regulatory race to the bottom. Thirdly, the incompatibility of the borderless character of data with the concepts of territorial data sovereignty leads to disjunctive implementation and a legal ambiguity that follows. This paper has identified that the European Union, in its GDPR policy and India, in its Digital Personal Data Protection Act (2023) policy are all necessary, but are still reactive and geographically delimited, thus failing to curtail the pervasive role played by globalized data processing. Finally, privacy must be preserved, which means that the paradigm shift is a better global collaboration, the unification of international standards, and providing corporations with strong accountability measures, which will result in the benefits of a connected world not being at the expense of fundamental human rights.

Keywords: Globalization, Data Privacy, Surveillance capitalism, Jurisdictional Arbitrage, Data Sovereignty, GDPR.

I. Introduction

The contemporary world has been forever imprinted by globalisation that is an ever-changing phenomenon inextricably tied to the liberalisation of trade, integration of markets, and free flow of capital and ideas throughout the world. It has the strongest effects in the digital world where technological interconnectedness is not limited by geographical frontiers. However, this connectedness has its price as it kills personal privacy. In the era of information, personal

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

information has often been termed as the new oil, which drives business strategies, governing systems, and even political predictions. Globalisation has placed personal information in a predicament of globalization and has put people in a continuum of personal dangers including identity theft, financial frauds, intrusive surveillance and manipulative behaviour targeting.

The problem has taken on an increased importance in India in terms of the exponentially growing internet penetration, the rise of multinational digital corporations, and the growing dependence on digital infrastructure. The right to privacy is listed among the basic rights that are entrenched in the constitution. in K.S. Puttaswamy v. Union of India[1] was one of the watershed moments. However, the following events like the Pegasus spyware scandals[2] and the current discussions about the idea of data localisation do show that constitutional recognition is not all. Globalisation of data flows raises very deep questions on the issues of jurisdiction, accountability and enforcement.

In this paper, the author will explore the idea of globalisation as a menace to data privacy. It argues that although globalisation has certainly led to innovation and economic growth, it has also led to a loss of individual autonomy as now individuals This is an exploitable phenomenon by both state and non-state actors. due to the ability to access personal data across the borders. Part II presents the conceptual model of how globalisation and privacy are related with each other. Part III compares the relative approaches and concentrates on the nature of the European Union, which is the General Data Protection Regulation (GDPR), the United States, the disjointed regulatory model, the state-centric nature of China, and other jurisdictional regimes.

Part 4 critically evaluates the Indian law with a focus on the constitutional developments and the statutory provisions these include the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023.[3] Part V gives case studies that help shed light on the physical impact of globalisation on privacy. Part VI ends by making policy proposals on how to balance privacy protection in the globalised era.

II. Conceptual Framework of Globalisation and Right to Privacy

A. Understanding Globalisation

The process of globalisation has been described as the augmentation of global social relations that connect localities far apart in such a manner that events taking place in localities are influenced by actions happening miles away and vice versa[4] in the economic field. In the technological context, globalisation is the spread of digital networks, internet initiatives and cloud infrastructure which has no territorial boundaries. The social media, the expansion of e-commerce across borders, and the creation of digital financial systems can be used to reflect the deep penetration of the globalised digital economy.

As globalisation allows the innovation process and the exchange of cultures, it has also brought criticism in destroying state sovereignty.[5] Traditional forms of governance are confined within territorial boundaries, but the boundaries are what have been blurred by the forces of globalisation. An example of this is where someone in India can post personal information to a site that is based in the United States, and is then stored on servers, which are located in Singapore, and processed in algorithms that are written in Ireland. This complexity in organization makes it hard to assign responsibility and accountability.

B. The Conceptual of Privacy in Laws and Jurisprudence

As a separate category of law, the concept of privacy has been evolving significantly during the last century. The phrase privacy originated

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

withThe right to privacy was first defined as the right to be left alone in a seminal article by Samuel Warren and Louis Brandeis in 1890, in their article, The Right to Privacy; since that time scholars have expanded the term to include many other related concerns, most specifically the concept of decisional privacy. (of having control over personal decisions). Daniel Solove also objected to the monolithic viewpoint on privacy by asserting that it is a "family resemblance" of correlated evils, such as surveillance, information processing, and data aggregation, rather than being a unitary concept.[7]

Coming to the Indian constitutional legislation, the right to privacy was not provided at first in the case of M. P. Sharma v. Satish Chandra[8] and Kharak Singh v. State of

U.P.[9] Nevertheless, a constitutionques case of Puttaswamy led a 9-judge court of the Supreme Court easily to identify the right to privacy in Article 21, clearly and explicitly defining the definition of informational privacy as substantive element of Some of the pillars of the ethical theory are human dignity and autonomy..[10]

Privacy is becoming a major human right in the international law system. Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) states that no person shall be arbitrarily interfered with in relation to his or her privacy, family, domicile, or correspondence.

This protection is restated in Article 17 of the 1966, International Covenant on Civil and Political Rights (ICCPR). Additionally, the Court of Human Rights has interpreted Article 8 of the European Convention on Human Rights (ECHR) to have serious repercussions on privacy. rights in many of its decisions, and Article 8 has been applied in many decisions as an instrument to enforce the normative character of privacy into the European human rights system.[11]

C. Privacy in the age of Datafication

The digital era has driven the issues of privacy to informational losses instead of physical invasions. "The surveillance capitalism theory" by Shoshana Zuboff sheds light on the manner in which companies turn personal information into a business opportunity to forecast and manipulate user behaviour and make a profit off of it[12]. This commodification is also enhanced by globalisation since multinational corporations do business in jurisdictions with different regulatory structures.

Data flows are currently transnational in nature. The cloud computing infrastructure, mobile applications and international payment systems all rely on a smooth cross- border transfer. Still, such globalised construction tends to exclude the personal consent and weakenes the control of regulations. This imbalance in power between the data subjects and the data controllers is increased by the fact that the local laws might not apply to other corporations or states in the world.

D. Tension Between Globalisation and Privacy

The tension between globalisation and privacy occurs in several forms:

1. **Jurisdictional Conflicts** - States are finding it difficult to attempt to give jurisdiction to foreign firms which are profiling their citizens. This is raised quite visibly when we considered the Safe Harbour vs. Privacy Shield litigations between the EU and the US.[13]

2. **Regulatory Arbitrage**: Corporations usually take the advantage of a loosener regulatory regime to handle and monetise personal data. As an illustration, data processing can be outsourced to jurisdictions that have lenient privacy laws.

3. **Mass Surveillance:** This has allowed states to cooperate in terms of intelligence sharing, akin to the "Five Eyes Alliance"[14], which is a product of Globalisation. The Snowden

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

disclosure concerning the national security agency of the US brought to the fore how cross-border surveillance, which can interfere with privacy of foreign nationals.

4. **Digital Colonialism:** Scholars have stated that as a result of the ability of globalisation to enable the use of technology-heavy states and companies to take control of data assets of developing nations, "digital colonialism"[15] has taken place.

Therefore, the globalisation of such connectivity only deepens the loss of informational self-determination - the right of individuals to decide how their personal information is gathered, used and distributed.

III. Globalisation and Data Privacy - Comparative Perspectives

Globalisation has established a data environment that is borderless and in which data transfers freely across jurisdictions. The legal mechanisms of privacy are, however, very disjointed. The approaches taken by different states are varied, depending on historical, cultural and political backgrounds. These models exhibit common potentials and pitfalls of globalisation in ensuring data privacy as illustrated in a comparative analysis of the models.

European Union:

The Gold Standard of Data Protection. The EU has essentially established the privacy laws in the global arena. The GDPR has been generally claimed to be the gold standard since 25 May 2018[16]. It sets out some fundamental principles, such as lawfulness, fairness, transparency, purpose limitation, data minimisation and accountability and provides people with real enforceable rights, such as the right to be forgotten, data portability and the right to object to automated decisions.[17] It also addresses the issue of using cross-border data flows: Chapter-V provides that you can only export personal data out of the EU when the destination country

provides an adequate level of protection[18]. This is why we have the emergence of such tools as standard contractual clauses (SCCs) and binding corporate rules (BCRs) to ensure that data flows without invading privacy.

But it's not a perfect machine. Such instances as Schrems I and II compelled the CJEU to invalidate the US Safe Harbour and Privacy Shield framework due to the lack of sufficient protection against the US surveillance practices[19]. These decisions demonstrate the fact that a powerful legal system can be questioned by the sophistication of international information flows.

U.S: Sectoral and Market-driven Approach:

The US does not have a single federal law on privacy as the EU. Rather, it is based on a patchwork of industry laws, HIPAA (Health Insurance Protability and Accountability Act) on health, GLBA (Gramm-Leach-Billey) on finance and the COPPA (Children's Online Privacy Protection Act)[20] on children data, etc. The market-based feel implies that privacy is addressed more as a consumer protection point than the right to it, which leaves companies with a wide margin.

The US model is highly influenced by innovation and free markets orientation. Privacy is addressed as a consumer-rights issue, instead of being a fundamental right[21]. Such a disjointed structure provides businesses with a great deal of room to gather and sell personal information. The emergence of a new business model, the so-called surveillance capitalism, including such names as Facebook and Google, throws the weakness of the purely market-driven approach.[22]

Globalisation can only aggravate these problems. The Snowden leaks revealed that the NSA was involved in mass surveillance of both Americans and foreigners, and this information caused global distrust.[23] In the absence of a

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

federal law that is analogous to the GDPR, data flows across the Atlantic have effectively stagnated as they have been left with insufficient mechanisms, such as SCCs.

China: State-Centric Model of Data Sovereignty:

The Chinese strategy is completely the opposite of the West. They prioritize state sovereignty and national security first, and the Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (PIPL, 2021)[24] are all rather strict. In other words, you are obliged to store all that personal data on Chinese soil in case you are operating a critical information infrastructure in China.[25]

The PIPL (Personal Information Protection Law), 2021 is also typically lumped with the GDPR, and it provides individuals with the rights to read, update, or erase their data. Nevertheless, the Chinese laws provide the state with enormous surveillance tools.[26] The entire balance indeed leans towards serving the interests of the government which is understandable due to the political climate in China. This is literally a nightmare to multinational companies in an ever-globalised digital economy they must comply with localisation regulations in China, with disclosure regulations, even where these conflict with the laws in other jurisdictions.

Brazil: GDPR-Model of Latin America:

Brazil launched the Lei Geral de Proteção de Dados (LGPD) in 2020, and it is a more or less direct copy of the GDPR.[27] It becomes internationalized - it is even impossible to hide the fact that it refers to any personal information which is done in Brazil or concerning individuals

located in Brazil, irrespective of where the processor is established.[28] The law gives individuals some rights:

i. The right to confirmation
ii. The right to access
iii. The right to make correction
iv. The right to data portability

Since Brazil is among such large emerging economies, the fact that it adopted GDPR- like regulations indicates how globalisation drives the convergence of regulations. Nevertheless, there exist challenges of enforcement in the view of institutional limitation and lack of capability to enforce it.

E. ***Other International Instruments and Jurisdictions***

Different countries have strived to strike a balance between globalisation and privacy. A good example of a regulatory framework aimed at balancing consumer protection and commercial interests is the Personal Information Protection and Electronic Documents Act (PIPEDA) balances consumer protection with business interests.[29] The Protection of Personal Information Act (POPIA) of South Africa equally includes a significant number of principles based on the General Data Protection Regulation (GDPR).[30]

Internationally, the examples of concerted harmonisation efforts are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, first promulgated in 1980 and later revised in 2013, and the APEC Privacy Framework, adopted in 2004.[31] However, these tools are soft law, and they do not have enforcement mechanisms.

F. ***Comparative Analysis:***

The three salient insights that are gained out of this comparative survey include:

i. **Fragmentation** - The European Union is a complete regulatory paradigm, the United States, China, and other jurisdictions are substantively different, which creates a strong fragmentation of data protection regulation.

ii. **Global Spillovers** - Barnes are decisions made in one jurisdiction that will have an effect elsewhere, such as the Schrems II case of the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Court of Justice of the European Union that has an impact on the operations of enterprises in the international arena.

iii. **Harmonisation need**- Due to Globalisation, transnational strategies are required; but the lack of an international treaty on data privacy creates gaps which are taken advantage of by the states and companies.

Here, therefore, globalisation is a paradoxical process that promotes both convergence, which is demonstrated through the spread of GDPR principles, and divergence, which is manifested through the increase in models that are competitive and state-focused.

IV. The Indian Legal Framework on Data Privacy

1. Constitutional Foundations

The establishment of privacy as a constitutional right in India has been significant in the development of norms of data protection. In Justice K. Puttaswamy (Retd.) v. Union of India, the right to privacy was determined to be a primary right in Article 21, and thus information privacy is positioned to be one of the fundamental aspects of personal dignity and autonomy.[32] This precedent case did not only rely on comparative jurisprudence, but it also set up a clear constitutional requirement on protecting personal data.

In the past, issues relating to privacy were scattered in cases like PUCL v. Union of India where procedural protection against telephone tapping[33] was introduced by the Court. Similarly, in District Registrar and Collector, Hyderabad. The Court held that

warrantless access to private records was invalid and the practice of warrantless access to such records was strengthened in Canara Bank, which had an impact on principles of informational privacy before the Puttaswamy[34] decision.

As a result, the constitutional framework entrenches privacy in the wider protection of life and personal liberty making it a necessary condition that any violation of such rights must be in line with the principle of legality, necessity, and proportionality.

2. Statutory Framework

1. ***Information Technology Act, 2000***

Information Technology Act, 2000, which is a law mainly enacted to support electronic commerce, has only few clauses that relate to data protection. Section 43(A) sets up an obligation of corporate entities to protect sensitive personal data, but Section 72(A) prosecutes the disclosure of data in unauthorized form.[35] However, these legal provisions are limited in scope and lack powerful tools of efficient enforcement.

2. ***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011***

The SPDI (Sensitive Personal Data or Information) Rules was the first attempt made by India to formalise the principles of data protection. They provided specifications on consent, notice and disclosure in collection and processing sensitive data. However, their very limited relevance to the corporates, as well as the limited punitive actions, minimized their efficiency.[36]

3. ***Digital Personal Data Protection Act, 2023***

The DPDP Act is the first data protection law in India that puts into law the principles of consent, limited purpose, minimisation of data, and accountability.[37] It also creates the Data Protection Board of India to adjudicate breaches. Although the Act largely resembles the GDPR, one of its aspects can be viewed as a major failure, as Section

17 offers excessive exemptions to the State, which brings up the issue of surveillance and

the erosion of personal freedoms.[38]

3. Digital Intervention

The judicial system has proceeded to extend privacy jurisprudence since Puttaswamy. In Aadhaar case (K.S. Puttaswamy v. In Union of India, 2019), the Supreme Court affirmed the Aadhaar scheme, but repeated that the provisions that required Aadhaar authentication to be given by private corporations would be invalid based on privacy considerations.[39] In Anuradha Bhasin v. Union of India, the Court highlighted the importance of proportionality in limitation of access to internet websites and supported the idea of privacy as a right on the internet.[40]

In the High Court level, there are cases like Karmanya Singh Sareen vs. Union of India . The emergence of transnational corporations such as WhatsApp and Facebook has challenged Union of India, and this demonstrates the inability of the Indian pre- DPDP structure to deal with globalised privacy harms.[41]

4. Policy Developments and Data Localisation

The data localisation campaigns in India are the best illustrations of globalisation impact on domestic policy-making. The fact that the payments information is to be stored at the national territory[42] per the directive of Reserve Bank of India and the propositions of the Draft E-commerce Policy (2019)[43] highlight an accentuating interest in the notion of data sovereignty. On the one hand, these measures are supposed to protect the privacy of the citizens and their national security, on the other hand, they have been criticized as the reason why the state can spy, as well as be used as a tool of trade protectionism.

5. Persistent Gaps

Irrespective of these changes, there are still a number of issues in the data privacy system in India:

i. **Broad State Exemptions:** Under Section 17 of the DPDP Act, broad access by the government is allowed.

ii. **Weak Institutional Mechanisms:** The Data Protection Board is not as independent as the EU system of supervisory authorities.

iii. **Enforcement Deficit**: India still faces a challenge of poor technical and legal infrastructure that can be used to implement privacy rights.

iv. **Digital Divide:** Inadequate awareness and access to digital literacy denies the full and fair exercise of the right to privacy to very large groups of the population.

V. Globalisation, Corporate Power and Privacy Risks

A. The Rise of Big Tech in India

Globalisation has eased the dominance of multinational companies, such as Google, Meta (previously Facebook), Amazon, and Microsoft, in the Indian digital realm. These organizations gather a lot of personal information about Indian users through search engines, online shops, cloud computing, and social networks. The subsequent hegemony poses significant material issues on the monopolisation and exploitation of data.

The case of Karmanya Singh Sareen v. Union of India[44], where Delhi High Court questioned the WhatsApp policy of sharing user data with Facebook after it was acquired. It was argued by petitioners that these practices violated privacy rights given the asymmetric bargaining positions between corporations and individual users. Even though the Court decided to abide by the current regulatory controls, the verdict highlighted the cross-border power of international businesses and their ability to transform privacy standards in India.

B. Corporate Surveillance and Informational Asymmetry

Corporations often use invasive practices that

include behavioural profiling, targeted advertising, and algorithm manipulation. The concept of surveillance capitalism presented by Shoshana Zuboff demonstrates that companies commodify individual information, which is the raw material of predictive analytics[45].

In Indian context the practices are reflected in the form of targeted political advertisements during the electoral periods hence raising democratic concerns. The Cambridge Analytica scandal, involving the misuse of Facebook information about Indian users, is an illustration of the danger of corporate exposure of global data streams.[46]

C. Data Breaches and Corporate Negligence

There have been several high-profile data breaches by international and local companies in India. A case in point is the 2018 Aadhaar data breach, that many media houses reported, revealing the vulnerability of how sensitive data related to over 1.1 billion citizens were handled.[47] Similarly, attacks on AirIndia, BigBasket, and MobiKwik demonstrated the magnitude to which worldwide digital environments amplify the threat of privacy.[48]

Lack of strict liability and enforcement procedures has given corporate actors the feeling of impunity thus promoting negligence.

D. State–Corporate Nexus and the Threat of Surveillance

The lines of corporate and state surveillance have been blurred by globalisation. Data acquisition and monitoring is a regular activity of government relying on corporate infrastructure. The Pegasus spyware scandal is an example of this phenomenon. In the case of Manohar Lal Sharma v. of Union of India[49], petitions were filed over the surveillance of Indian citizens, such as journalists and activists, using Pegasus, built

by the Israeli NSO Group.[50] The Supreme Court later established a committee of experts to conduct research recognizing the grave concern to privacy and democratic rights.

This nexus explains how globalisation allows foreign technologies of surveillance to be imported into India, thus potentially undermining the constitutional protections of privacy.

E. Digital Colonialism and Power Imbalances

Researchers refer to the presence of global technology giants in the Global South as digital colonialism. In India, this is in the form of harvesting of user data without proper compensation or regulation. Introduction of standardised global privacy policies often sidelines domestic interests, thus making Indian users susceptible.

The Aadhaar project has been criticized in this respect itself. Though Aadhaar is a state project, its utilization of international biometric solutions and commercial contractors highlights the interconnection between globalisation and national privacy threats. Opponents argue that Aadhaar is a techno-solutionist model that has been imported into the global space and not adjusted to Indian circumstances.[51]

F. The Chilling Effect on Civil Liberties

The effect of corporate and state surveillance aided with international technologies is a chilling influence on civil liberties. Self-censorship of online activity is often practised by users due to the fear of possible surveillance, thus undermining the rights guaranteed in Articles 19 and 21 of the Constitution. The Supreme Court recognized this chilling effect in the case of Anuradha. Union of India, in which the Court highlighted that freedom of speech cannot be limited by means of limitless restrictions to access of internet.[52]

VI. Conclusion

Globalisation has immensely changed the structure of informational exchange, provincing

traditional borders and creating a hyper-connected digital ecosystem. On the one hand, it has enabled the largest economic growth and technological advancement in history, as well as the transnational cooperation of people; on the other hand, it is also putting at risk one of the most essential human rights the right to privacy. In this new digital era, personal information is not only a marketed commodity, but it also acts as a coercive tool, and not only by governments, but by companies as well.

A review on the impact of globalisation on data privacy paints a subtle dilemma between economic liberalisation and protection of human rights. Globalisation encourages the free circulation of information but this circulation is usually one way only: it gives more and more advantages to those who are technologically and financially powerful and marginalises those whose information supports these structures. The collection, processing, and transfers of personal data across borders without any regulations have made the current privacy protection measures mostly useless.

The judicial development that led to the case of Just Powell v. India in the Indian context. Privacy has been proclaimed a necessary element of human dignity by Union of India in Article 21 of the Constitution. However, the application of this right still is scattered in the forces of international trade, technological addiction, and business interests. The Digital Personal Data Protection Act of 2023 is a promising move but still grapples with cross-border data flow issues, governmental exemptions, and the lack of an independent oversight organs.

On the global scene, the absence of binding international data protection regime continues to create disparities and gaps in regulations. Current tools like the OECD Guidelines and the APEC Framework have normative guidelines but lack effective accountability. As a result, various multinational companies have taken advantage of the jurisdictional differences and have played the jurisdictional arbitrage game to avoid strict compliance costs.

To advance, a rights-based global data governance system should be designed on the basis of equity, accountability and reciprocity. As a data and technologically vibrant country, India can use this as its opportunity to lead in endorsing a Global Privacy Compact A global treaty that will synchronize international data flows with human- rights principles. A framework like this should institutionalise the principles of informed consent, data minimisation, transparency in algorithms and enforceable cross-border responsibility.

After all, the need to maintain privacy in the globalisation age requires more than a shift in legislation; it requires an act of moral and political will to pursue human dignity in the digital realm. The concept of privacy has to be rethought as not a challenge to innovation but rather the foundation of trust that lies at the core of the global digital economy. As the world enters into greater depths of a data driven century, the issue of protecting privacy will decide not only the course of individual agency, but the validity of democratic governance itself.

Bibiliography

Books

1. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013).

2. David Lyon, *Surveillance Studies: An Overview* (Polity Press, 2018).

3. Graham Greenleaf, *Global Data Privacy Laws 2023: Fifty Years of Privacy Development* (Privacy Laws & Business International Report, 2023).

4. Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012).

5. Luciano Floridi, *The Ethics of Artificial Intelligence* (Philosophy & Technology, 2019).

6. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of

Anonymization" (2010) 57(6) *UCLA Law Review* 1701.

7. R. Deibert, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi, 2020).

8. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

Journal Articles and Reports

9. Arghya Sengupta, "Data Privacy and Economic Growth: The Indian Paradox" (2022) 18(1) *Indian Journal of Law and Technology* 45.

10. K. S. Park, "Cross-Border Data Flow and Data Protection" (2018) 21(2) *Journal of International Economic Law* 351.

11. S. Aaronson, "Data is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows" (2019) *CIGI Paper No. 197.*

12. S. Ramesh, "Cambridge Analytica and Indian Elections: A Privacy Wake-Up Call" (2019) 54(10) *Economic and Political Weekly* 22.

13. UNCTAD, *Digital Economy Report 2021: Cross-Border Data Flows and Development* (United Nations, 2021).

14. UNCTAD, *Global Data Governance: Policy Brief No. 94* (2022).

15. G20 Digital Economy Working Group, *Bali Principles on Data Free Flow with Trust* (2022).

Cases

1. Google LLC v. Competition Commission of India (2023) SCC OnLine CCI 4.

2. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

3. WhatsApp LLC v. Union of India (2021) SCC OnLine Del 5256.

Statutes and Rules

4. Information Technology Act, 2000.

5. The Digital Personal Data Protection Act, 2023.

6. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

7. General Data Protection Regulation (EU) 2016/679.

8. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Article 14.11.

Government Documents and Policy Papers

9. Ministry of Home Affairs, *Manual on Mutual Legal Assistance in Criminal Matters* (2020).

10. Ministry of Electronics and Information Technology (MeitY), *National Data Governance Framework Policy* (2022).

11. NITI Aayog, *Discussion Paper on Data Empowerment and Protection Architecture* (2020).

International Instruments

12. Universal Declaration of Human Rights, 1948.

13. International Covenant on Civil and Political Rights, 1966.

14. OECD, *Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).

15. APEC, *Privacy Framework* (2015).

Online Sources

16. Internet Freedom Foundation, "DPDP Act 2023: An Analysis" (2023) https://internetfreedom.in accessed 5 October 2025.*The Wire*, "Pegasus Project: How India Was Targeted" (2021) https://thewire.in accessed 5 October 2025.

ENDNOTES

1 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

2 Manohar Lal Sharma v. Union of India, (2021) 10 SCC 275

3 Ministry of Electronics and Information Technology, Draft National E-Commerce Policy (2019).

4 Anthony Giddens, The Consequences of Modernity (Standford University Press, 1990) p. 64

5 Saskia Sassen, Losing Control? Soverenity in an Age of Globalisation (Columbia University Press,1996) p. 12.

6 Samuel Warren and Loius Brandeis, "Right to Privacy" (1890) 4 Harvard Law Review 193

7 Understanding Privacy (Harvard University Press,2008) p. 25

8 AIR 1954 SC 300.

9 AIR 11963 SC 129.

10 Justice K.S.Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

11 S. and Marper v. United Kingdom, (2008) ECHR 1581.

12 The Age of Surveillance Capitalism (Profit Books,2019).

13 Schrems v. Data Protection Commissioner, Case C-362/14, Court of Justice of EU, 2015.

14 Edward Anowden, Permanent Record (Metropolitan Books,2019).

15 Michael Kwet, "Digital Colonialism: Us Empire and New Imperalism in the Global South" (2019" 20 Race & Class 1.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Genera Data Protection Regulation).

17 Ibid., arts. 15-22

18 Ibid., ch. V

19 Schrems v. Data Protection Commissioner, Case C-362/14, CJEU (2015); Data ProtectionnCommissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, CJEU (2020).

20 Paul M. Schwartz & Daniel J. Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102 California Law Review 887.

21 Daniel J.Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy" (2014) 114 Columbia Law Review 583.

22 Shoshana Zuboff, The Age of Surveillance Capitalism (Profit Books,2019).

23 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State (Metropolitan Books,2014).

24 Cyber Security Law of the People's Republic of China,2017; Data Security Law,2021; Personal Information Protection Law,2021.

25 Personal Information Protection Law, 202, art. 40.

26Samm Sacks, " China's Emerging Data Privacy System and GDPR" (2018) New America Report.

27 Lei Geral de Protecao de Dados (Law No. 14,709/2018), effective 2020

28 Ibid., art. 3.

29 Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 (Canada).

30 Protection of Personal Information Act 4 of 2013 (South Africa).

31 OECD, Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (2013).

32 AIR 2017 10 SCC 1.

33 AIR 1997 1 SCC 301.

34 District Registrar and Collector, Hyderabad v. Canara Bank, (2005) 1 SCC 496.

35 Information Technology Act, 2000, ss. 43A and 72A.

36 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

37 Digital Personal Data Protection Act, 2023, No. 22 of 2023.

38 Apar Gupta,: India's Digital Personal Data ProtectionAct: A Critical Appraisal" (2023) 58 (4) Economic & Political Weekly 15.

39 K.S. Puttaswamy v. Union of India (Aadhar), (2019) 1 SCC 1.

40 Anuradha Bhasin v. Union of India, (2020)3 SCC 637.

41 Karmanya Singh Sareen v. Union India, (2017) 8 SCC 128

42 Reserve Bank of India, Storage of Payment System Data (Notification, 6 April 2018).

43 Ministry of Commerce and Industry, Draft National E- Commerce Policy (2019)

44 Karmanya Singh Sareen v. Union of India, (2017) 8 SCC 128.

45 Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books, 2019).

46 Ravi Agrawal, "The Cambridge Analytica Scandal in India" (2018) Foreign Policy

47 Rachna Khaira, "Rs. 500, 10 Minutes, and You Have Access to Billion Aadhaar Details" The Tribune(4January 2018).

48 Internet Freedom Foundation, "Data Breach Tracker: Documenting India's Growing Data Crisis" (2021)

49 (2021) 10 SCC 275.

50 Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South" (2019) 20 Race & Class 1.

51 Reetika Khera, "Aadhaar: An Uncertain Future of Welfare" (2019) 54(13) Economic & Political Weekly 18.

52 (2020) 3 SCC 637.