VOLUME 10 ISSUE 1 ARTICLES & ESSAYS

University of Bologna Law Review

https://doi.org/10.6092/issn.2531-6133/22377

Received: 10 Nov. 2024 | Reviewed: 25 Jun. 2025 | Accepted: 26 Jun. 2025 | Published: 21 Oct. 2025

Data Privacy Across Borders: A Comparative Analysis of European Union and Indian Protection Laws

ANITA YADAV* & RABIKANT PANDEY**

*Anita Yadav (corresponding author) is an Assistant Professor of Law (Senior Scale) at the Campus Law Centre, Faculty of Law, University of Delhi (India). She has completed her LL.M. and Ph.D. from the National Law School of India University (NLSIU) (India). During her Ph.D. programme she was an Erasmus Mundus Scholar at University of Göttingen (Germany). Her research focuses on Human Rights, International Humanitarian Law, Environment Conservation and Artificial Intelligence & Law.

**Rabikant Pandey is an independent research scholar, holding an LL.B. and an LL.M. from the University of Delhi (India). His research focuses on Constitutional Law, Information Technology Law, and Criminal Law, with specific interest in the intersection of privacy, digital governance, and rights-based legal frameworks.

@ *ayadav@clc.du.ac.in **rabikant1209@law.du.ac.in

*0009-0005-4070-9748 **0009-0000-5603-0071

ABSTRACT

Cross-border data protection frameworks increasingly shape global digital governance as privacy rights intersect with economic imperatives. This article examines the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDP Act) through comparative legal analysis, evaluating their distinct approaches to international data transfers and privacy safeguards. The GDPR establishes privacy as a fundamental right through extraterritorial application and stringent adequacy mechanisms, while India's DPDP Act balances individual data protection with economic development objectives in one of the world's fastest-growing digital markets. This study employs doctrinal methodology and comparative legal analysis to explore privacy within the international human rights framework, emphasising personal data sovereignty as essential to human dignity. Drawing on surveillance theory and analysing the GDPR's adequacy mechanism against India's data localisation and cross-border transfer provisions, the research reveals significant divergences in regulatory philosophy and enforcement mechanisms. The analysis demonstrates that India's evolving engagement with global data protection standards positions it as a critical actor in developing harmonised international frameworks. The findings indicate that reconciling the EU's rights-based approach with India's development-oriented model requires adaptive governance structures that accommodate diverse regulatory contexts. This research contributes to understanding how divergent legal traditions can converge toward cooperative data governance, highlighting implications for international trade negotiations, digital sovereignty debates, and the architecture of future cross-border data transfer mechanisms that balance privacy protection with economic integration.

KEYWORDS

Cross-border, Right to Privacy, Data Protection, European Union, India

TABLE OF CONTENTS

INTRODUCTION

The transnational data movement has become crucial for enterprises, governments, and individuals in the contemporary globalised digital economy. Data, frequently referred to as the "new oil",[1] powers critical sectors ranging from finance and healthcare to e-commerce and social media.[2] Nonetheless, as data traverses borders effortlessly, apprehensions over privacy, security, and national sovereignty have converged. This has led to the institutionalisation of regulatory frameworks safeguarding personal data across several countries. In other words, it means safeguarding personal information from unofficial, unsanctioned, unapproved, and unauthorised use of data. At the same time, it ensures that individuals have control over their data. This concept is closely linked to informational autonomy, which states that individuals should be the sole deciding authority regarding the use of their data. Protecting this right is crucial for maintaining personal identity, dignity, and autonomy, especially in an era in which data has become a significant asset for corporations and governments.

Cross-border data protection pertains to the Regulation of personal data transfer across international boundaries. The proliferation of multinational enterprises, worldwide trade, and cloud-based services results in personal data often traversing jurisdictions with varying legal frameworks, posing substantial hurdles to ensuring uniform protection. These transfers provoke apprehensions regarding the sufficiency of privacy safeguards in the recipient nations and the possibility of data misuse, encompassing monitoring and economic exploitation.[3]

It must be stated that numerous international human rights documents have acknowledged Privacy as a fundamental human right. For instance, Article 12 of the Universal Declaration of Human Rights affirms the right to privacy, stating, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence".[4] Similarly, the International Covenant on Civil and Political Rights affirms the right to Privacy under Article 17, which prohibits unlawful interference with an individual's privacy, family, or correspondence.[5] Further in Europe, Article 8 of the European Convention on Human Rights [hereinafter E.C.H.R.] provides the foundation

[1] "Data is the new oil". It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc. To create a valuable entity that drives profitable activity, so data must be broken down and analyzed for it to have value" – Clive Humby, *see e.g.*, Nisha Talagala, *Data as The New Oil Is not Enough: Four Principles for Avoiding Data Fires*, Forbes (Mar. 4, 2022), https://www.forbes.com/sites/nishatalagala.

[2] *See id.*

[3] *See* U.N. Conference on Trade and Development, Data protection regulations and international data flows: Implications for trade and development (Apr. 19, 2016).

[4] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

[5] G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

for safeguarding the privacy of the individual while at the same time ensuring the reverence and dignity for private and family life, along with home and correspondence.[6] Additionally, the General Data Protection Regulation [hereinafter G.D.P.R.] establishes data protection as a fundamental right in the European Union [hereinafter E.U.], safeguarding personal data within and beyond E.U. borders. It also provides the international benchmark for privacy regulation, influencing data security/protection legislation internationally.[7]

India has been recognised as one of the world's rapidly growing digital economies and occupies a vital role in these discussions. Balancing economic growth with innovation and digital sovereignty, while at the same time institutionalising the framework for safeguarding and respecting individual privacy and national security, presents a significant challenge, especially amid the rapid expansion of its technology sector and increasing volumes of cross-border data exchanges. In this scenario, the D.P.D.P. Act of 2023 highlights an essential step towards securing personal data domestically, while also raising critical questions about the country's approach to regulating international data flow.[8]

The article begins by exploring the concept and development of privacy legislation in India and Europe, highlighting the significance of safeguarding personal information and its connection to human dignity. It offers a comparative and critical insight into the analysis of data security/protection laws in India and Europe, followed by an examination of the current trans- border or cross-border data security/protection rules. The article reviews data transfer regulations and the steps India has taken to protect individuals' private information during international exchanges. By analysing India's approach to cross-border data protection within the context of global data governance frameworks, such as the E.U.'s G.D.P.R., the article seeks to evaluate India's position on data flows, the challenges it faces, and its ambitions to emerge as a digital leader while ensuring the protection of its citizens' data.

[6]European Convention of Human Rights and Fundamental Freedoms [hereinafter E.C.H.R.], art. 8, opened for signature Nov. 11, 1950, C.E.T.S. No. 005.

[7]*See* Shravishtha Ajaykumar, Amoha Basrur & Vaishnavi Sharma,*The Digital Personal Data Protection Act 2023: Recommendations for Inclusion in the Digital India Act*, Observer Research Foundation (Oct. 30, 2023) https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023-recommendations-for-inclusion-in-the-digital-india-act.

[8]*See* Charru Malhotra & Udbhav Malhotra, *Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India*, 70 Indian J. Pub. Admin. 516, 516-20 (2024) (India).

1. CONCEPT OF PRIVACY AND DATA PROTECTION LAWS

1.1 UNDERSTANDING PRIVACY THROUGH INDIVIDUALISM

This article primarily addresses the individual's right to privacy and the need for data security/protection laws. It must be stated that the understanding of "individualism" plays a seminal role in shaping their concept of privacy. Individualism, as a social and political theory or ideology, is centred on affirming "the moral value of the individual".[9] According to the principle of individuality, each person, as a gift of life from God, is entitled to fully exercise all associated freedoms, including the right to privacy.[10]

The principles of human dignity and autonomy form the basis of fundamental individual rights, often described as natural rights. These rights are viewed as intrinsic, and existed before any governmental or legal systems. Philosophers like John Locke and Jean-Jacques Rousseau asserted that individuals possess an inherent right to freedom from oppression, encompassing personal freedom, property rights, and liberty. Locke listed life, liberty, and property as core natural rights. Privacy is integral to freedom, even if not stated. The protection of one's personal space, thoughts, and choices underlies the concept of individual liberty and aligns closely with the natural rights framework.[11]

1.2 EARLY LEGAL CONCEPTION OF PRIVACY

In the legal realm, Samuel Warren and Louis Brandeis are credited with providing the first explicit definition of privacy in American legal history, famously advocating for "the right to be let alone". They argued that the law should offer criminal and civil protections to safeguard individuals' "inviolate personality" from state interference. In light of the rise of intrusive technologies and sensationalist journalism, scholars like Warren and Brandeis think that individuals should be the sole authority over their personal information and private lives.[12]

The concept of privacy traces its origins to biblical times and carries multiple interpretations. Privacy can be understood in various ways: as a right to private property, as ownership over one's name and image, as control over one's personal and financial matters, as the confidential operations of an organisation, or as the protection

[9] Steven Lukes, *The Meanings of "Individualism"*, 32 J. Hist. Ideas 45 (1971).
[10] *Id.* at 46.
[11] *See* John Locke, Two Treatises of Government 45-66 (Peter Laslett ed. Cambridge Univ. Press 1988) (1690) (U.K.).
[12] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193-202 (1890).

of intimate and family life. Privacy thus encompasses a broad range of meanings, each significant. Individuals use it daily in various circumstances to criticise others, society, and the state. In his seminal paper "Privacy and the Law: A Philosophical Prelude", Milton Konvitz articulates these concepts as follows:

> Once a civilization has made a distinction between the "outer " and the "inner" man, between the life of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between the realm of God and the realm of Caesar, between Church and State, between rights inherent and inalienable and rights that are in the power of government to give and take away between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called the idea of a private space in which man may become and remain himself.[13]

Alan Westin states privacy has four characteristics: seclusion, closeness, anonymity, and restraint. According to Westin, being alone is to be physically apart from other people. An intimate relationship develops when two or more people are alone, characterized by closeness, comfort, and candor. In cases of public privacy, people want to remain anonymous. At its core, reserve is about protecting one's mental space from prying eyes; it's about asking people to respect one's wishes regarding the degree to which they divulge private information.[14]

1.3 THE SHIFT FROM PHYSICAL TO DIGITAL SPACES

In our digital era, privacy has taken on new dimensions. As we go from physical to digital platforms, personal data, including chat histories, online behaviour, financial details, and biometric information, is continually being gathered, analysed, and occasionally used—without people's awareness or agreement. Nowadays, the right to privacy goes beyond only controlling one's own destiny and living space. The authority over the personal data and information in the digital realm has become increasingly essential, especially with the advent of "big data" and the "Internet of Things", which have greatly amplified the value of such data. The lack of robust data protection regulations has led to the unauthorised access and misuse of personal information, frequently resulting in

[13] Milton R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31 L. & Contemp. Probs. 272, 273 (1966).
[14] *See* Leon A. Pastalan, *Privacy as a Behavioral Concept*, 45 Soc. Sci. 93, 94 (1970).

privacy violations, and at the same time, has become the basis of trust erosion between individuals and businesses.[15]

Since the beginning of the internet and social media, there has been an unprecedented accumulation, exchange, and examination of personal data, and governments throughout the globe are enacting Data Protection Laws to protect individuals' privacy and forestall exploitation. Websites started keeping tabs on users' movements throughout the internet using tracking technology like cookies, collecting information about their preferences and how they browse. Initially, this data was used to enhance user experiences. However, it soon became clear that personal information might be used for commercial purposes.[16]

1.4 RISE OF DATA MONETISATION AND SURVEILLANCE

A turning point in privacy discussions came with personal data monetisation. The development of business models by multinational firms based on collecting, analysing, and selling user data raised serious concerns about the exploitation of personal information for profit. There have been calls for more transparency and control over personal data because many people were unaware of how companies collected and used their data.[17] Social media has significantly reshaped perceptions of privacy. Platforms like "Facebook", "Instagram", and "Twitter" allow individuals to effortlessly share personal experiences, photos, and opinions with a vast audience. Unlike the traditional view of privacy as the safeguarding of one's personal space, more people today are voluntarily sharing information that was once considered private.[18] However, social media companies often collect and store far more data than users realise, including location data, browsing habits, and conversation patterns, even if users may wish to disclose personal information. Problems arise when individuals do not always have complete control over how their data is used after sharing, especially when data breaches and algorithmic manipulation are prevalent in the social media world.[19]

---

[15] *See generally* Adam Henschke, *Privacy, the Internet of Things and State Surveillance: Handling Personal Information Within an Inhuman System*, 7 Moral Phil. & Pol. 123, 123-35 (2020).

[16] *See* Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, Harvard Business Review (May, 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[17] *See id.*

[18] *See generally* Stefan Stieglitz et al., *Social Media Analytics – Challenges in Topic Discovery, Data Collection, and Data Preparation*, 39 Int'l J. Info. Mgmt. 156, 157 (2018) (U.K.).

[19] *See id.* at 159.

If data alterations are made and observed repeatedly, the human mind will respond accordingly; individuals may accept false data as truth and act in a specific manner. The 2018 Cambridge Analytica scandal highlighted the dangers of data misuse on social media, as the personal information of millions of users of Facebook was collected without their consent and utilised for targeted political maneuvering and advertising. The incident prompted enquiries over the ethics of data acquisition and manipulation in a context where privacy and personal information are seen as commodities.[20] Privacy is becoming recognised as an essential freedom in the digital age due to this case's direct attack on voters' liberty and damaging democracy. As digital technologies become increasingly pervasive, personal data control is essential to human dignity, autonomy, and freedom. Philosophers like Immanuel Kant have long argued "that individual autonomy and the ability to make choices free from external influence are central to upholding human dignity".[21] Lastly, in the digital era, the capacity to manage one's data is essential for preserving autonomy. Individuals relinquish authority over their information without privacy, leading to manipulation, surveillance, and potential harm.

2. INFORMATIONAL PRIVACY

2.1 DEFINING INFORMATIONAL PRIVACY

The concept of information privacy, or informational privacy, is relatively new. It is evolving as digital tools and networks have reshaped traditional understandings of privacy to encompass personal data rights. Informational privacy emphasises the individuals' authority and control over their private information and how others may use it. This underscores the need to protect diverse forms of data, including financial details, health records, communications, and identification information. At its core, informational privacy rests on the right to privacy, which prohibits unauthorised disclosure of personal data. Alan Westin defines informational privacy as the capacity of individuals to control the dissemination of their personal information to others.[22] Later studies conducted by Westin laid the groundwork for modern privacy notions,

[20] *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, The New York Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[21] *Kant's Social and Political Philosophy*, Stanford Encyclopedia of Philosophy (Apr. 11, 2022), https://plato.stanford.edu/entries/kant-social-political/.

[22] *See* Alan Westin, Privacy and Freedom 6 (1967).

demonstrating that people should possess control over their informational timing, manner, and the extent to which their data is shared with others.[23] There are presently two predominant conceptualisations of information privacy: the first perceives privacy as the capacity to "limit or restrict others from accessing information about" oneself, while the second defines privacy as the "control of personal information".[24] Both approaches are predicated on the assumption that information is a commodity that can be regulated or to which access can be limited. Data or information are generally considered objective entities that exist, a notion often accepted but rarely stated.[25] In the modern age, personal information has transformed into a commodity that is exchanged in the information marketplace and among data brokers. Personal information possesses monetary worth and can be regarded as a sort of property that individuals can own and negotiate within the economic and commercial realm.[26] Upon closer examination, if we associate personal information with property rights, others possess no entitlement to utilise our personal information without consent. This perspective is attractive, although it presents a problematic concept. To associate personal information with property rights, the owner must hold it; nevertheless, the essential question is how one can have an ethereal substance like information, which escapes physical control.[27] Consequently, personal data privacy cannot be equated with property, as, unlike tangible assets, data can be replicated and utilised by several individuals without diminishing its worth or utility. For instance, if an individual uses your data, it does not exclude others from accessing that same data. This differs from a tangible thing, such as a car, where simultaneous usage by multiple individuals is not feasible. Thus, considering personal data as property fails to fully reflect the inherent nature of data functionality.[28]

2.2 ESSENTIAL ATTRIBUTES AND DEMOCRATIC NECESSITIES

Informational Privacy possesses three characteristics: it's "nonrivalrous", "imperceptible", and "recombinant". Firstly, information is nonrivalrous, meaning that multiple individuals can utilise the same information concurrently without diminishing its availability to others. Secondly, data privacy breaches are challenging to identify due

[23] *See id.* at 35.
[24] Jens-Erik Mai, *Three Models of Privacy: New Perspectives on Informational Privacy*, 37 Nordicom Rev. 171, 171-72, (2016) (Swed.).
[25] *See id.*
[26] *See id.* at 173.
[27] *See* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 Berkeley Tech. L.J. 461, 464 (2000).
[28] *See id.*

to their often imperceptible nature. Information may be accessed, stored, and disseminated without prior notification. The capacity to traverse at light speed amplifies the obscurity of data access; "information acquisition can constitute the most rapid form of theft". Thirdly, since information is recombinant, data processing outcomes can be used again as input to create new data outputs. This cyclical process enhances the potential for ongoing analysis and the creation of new information.[29] Moreover, creating a robust data protection regime is essential; however, it is a complex undertaking that governments must pursue. It emphasises the necessity for the state to diligently strike a balance between protecting individual privacy and fulfilling other critical objectives served by data protection, while simultaneously taking into account the state's legitimate interests.[30]

In democratic countries, ensuring informational privacy is crucial for protecting individual liberties and rights. Privacy enables individuals to articulate their thoughts freely, make independent choices, and participate in democratic activities without excessive influence or monitoring. Privacy rules curtail the authority of both governmental and private organisations over personal data, thereby preventing the misuse of information that could manipulate public opinion or suppress opposition.[31]

3. EVOLUTION OF DATA PROTECTION LAW

3.1 INDIA

Although the Indian Constitution does not explicitly enshrine the right to privacy, the Indian Judiciary, notably the Supreme Court, has acknowledged privacy as both a fundamental constitutional right and a common law right since the 1960s. Despite consistently affirming this right, the Judiciary has not articulated a precise definition, instead opting for a case-by-case approach to delineate its contours. This Section examines key Supreme Court decisions that have progressively shaped the recognition and scope of the right to privacy, illustrating its evolution as a fundamental right within India's legal framework.

[29] *See* Justice K.S. Puttaswamy (Retd.) & Anr, v. Union of India & Ors., (2017) 10 SCC 1 (India).
[30] *See id.* at 179.
[31] *See id.*

3.1.1 EARLY JUDICIAL RELUCTANCE

The development of privacy jurisprudence in India commenced with the *M.P. Sharma* case,[32] in which the Supreme Court addressed privacy issues for the first time. A search and seizure carried out by police as part of a criminal investigation gave rise to this case. The Court decided that no constitutional requirements were violated by the authority to conduct searches and seizures. Furthermore, the Court stated the following to avoid acknowledging the right to privacy as a fundamental constitutional right:

> 17. In any system of jurisprudence, a power of search and seizure is an overriding power of the State for the protection of social security. That power is necessarily regulated by law. When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the Fourth Amendment, we have no justification to import it into a different fundamental right, by some process of strained construction. Nor is it legitimate to assume that the constitutional protection under Article 20(3) would be defeated by the statutory provisions for searches.[33]

The following significant case on the subject was the *Kharak Singh* case,[34] which raised concerns about whether the Uttar Pradesh Police Regulations permitted police surveillance. The petitioner claimed that this surveillance went against his constitutional rights as guaranteed by Articles 19(1)(d) and 21. The Supreme Court concluded that there was no fundamental right to privacy in a split ruling. Nonetheless, Justice Subba Rao acknowledged in his opinion that privacy is an essential part of individual liberty, adding that "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements but also free from encroachments on his private life".[35] Justice Subba Rao's dissent laid the foundation for recognizing privacy as an essential element of the right to personal liberty under Article 21 of the Indian Constitution.[36]

---

[32] M.P. Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors. (1954), SCR 1077 (India).
[33] *Id.* at 17.
[34] Kharak Singh v. State of Uttar Pradesh & Ors., (1964]),1 SCR 334 (India).
[35] *Id.* at 28.
[36] India Const. art. 21: **"Protection of life and personal liberty.**- No person shall be deprived of his life or personal liberty except according to the procedure established by law**".**

3.1.2 PROGRESSIVE EXPANSION THROUGH CASE-BY-CASE RECOGNITION

Subsequently, the *Govind* case[37] represented a significant advancement in Indian privacy legislation. The petitioner contested specific police regulations permitting the surveillance of repeat offenders. The Supreme Court determined that specific police regulations conflicted with the concept of personal liberty and recognized the right to privacy as a fundamental right within the Indian Constitution. However, it upheld that the right to privacy should develop progressively through individual cases, rejecting an absolute interpretation. The Court further noted the following points:

> 28. The right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India, and the freedom of speech create an independent right of privacy as an emanation from them, which one can characterize as a fundamental right, we do not think that the right is absolute.[38]

A similar assertion was affirmed by the Supreme Court in *R. Rajagopal* case,[39] where the Court examined whether a magazine's publication of a convicted prisoner's memoirs violated his right to privacy. The Supreme Court acknowledged the right to privacy in the context of the press and public figures. The Court further observed the following points:

> The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education, among other matters.[40]

This ruling marked a significant step in explicitly recognising privacy as a component of Article 21, asserting that the press is restricted from publishing unauthorised information about an individual's private life, except when the individual is a public figure or has willingly disclosed the information. Subsequently, in the *People's Union of Civil Liberties* case [hereinafter PUCL case],[41] the case addressed the matter of "telephone tapping". PUCL challenged the government's interception of telephone conversations,

[37] Govind v. State of Madhya Pradesh, & Ors., (1975) 2 SCC 148 (India).
[38] *Id.* at 28.
[39] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (India).
[40] *Id.* at 26.
[41] People's Union of Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).

arguing it violated the right to privacy. The Supreme Court responded with the following explicit statement:

> We have, therefore, no hesitation in holding that right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed except according to procedure established by law.[42]

3.1.3 PRIVACY AND PERSONAL IDENTITY

Furthermore, in the *Naz Foundation v. Government of NCT of Delhi*,[43] although the primary focus was L.G.B.T.Q.+ rights, the case also addressed the right to privacy. By decriminalising homosexuality under Section 377 of the Indian Penal Code, the Delhi High Court asserted that an individual's sexual orientation is fundamentally linked to personal privacy. The Court emphasised that "the right to privacy is intrinsic to the right to life and liberty guaranteed to the citizens of this nation by Article 21", underscoring that sexual orientation is a deeply personal aspect of privacy.[44] This case acknowledged privacy concerning individual sexual orientation, establishing a foundation for subsequent advancements in privacy legislation.

3.1.4 LANDMARK RECOGNITION: JUSTICE K.S. PUTTASWAMY

Finally, in the landmark case of *Justice K.S. Puttaswamy case*,[45] popularly called "Privacy Judgement", the Supreme Court interpreted privacy as a penumbral right under Article 21 of the Indian Constitution. The decision overturned the earlier rulings in the *M.P. Sharma* case[46] and the *Kharak Singh* case.[47] The unanimous verdict on privacy is a restatement of core constitutional principles. Justice D.Y. Chandrachud held that as follows:

> (A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. (C) Privacy is a constitutionally protected right that emerges primarily from guaranteeing life and personal liberty in Article 21 of the

[42] *Id.* at 17.
[43] Naz Foundation v. Gov't of NCT of Delhi, (2009) 111 DRJ 1 (India).
[44] *Id.*
[45] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).
[46] M.P. Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors., (1954) SCR 1077 (India).
[47] Kharak Singh v. State of Uttar Pradesh & Ors., (1964]) 1 SCR 334 (India).

> Constitution. (F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home, and sexual orientation. Privacy also connotes a right to be left alone. (H) Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law that encroaches upon privacy must withstand the touchstone of permissible restrictions on fundamental rights. (I) Privacy has both positive and negative content. The negative content restrains the state from intruding on a citizen's life and personal liberty. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.[48]

This Judgement made the right to privacy more essential and precious than any other right. Article 21 of the Constitution requires fair, reasonable, and just legislation that sanctions privacy violations. The Supreme Court's three-part test applies to any law that infringes on privacy. First, legality requires the law to be legal and statutory. Second, the measure must serve the legitimate government goal. The third requirement is proportionality; measures must align with the intended objective.[49] Therefore, every legislation that infringes upon individual privacy rights must be evaluated against the specified standards. The circumstances would have varied had privacy remained solely a statute or common law safeguard.

In his discussion on the right to informational privacy in the contemporary context, Justice D.Y. Chandrachud held that as follows:

> Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and implement a robust regime for data protection. Creating such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but

[48] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 SCC 1, at 459.
[49] *See id.* at 179.

> also some disadvantages. Access to information that an individual may not want to give needs the protection of privacy.[50]

The aforementioned cases demonstrate that privacy rights have taken time and effort to develop. The judiciary has progressively expanded its scope through constitutional interpretation. Initially, in instances like *M.P. Sharma* and *Kharak Singh*, the Supreme Court denied privacy as a fundamental right, but in K.S. Puttaswamy, it recognised and strengthened it.[51] Today, privacy is firmly identified as a fundamental right, protecting individuals against encroachments by state and non-state actors across various facets of life.

3.2 EUROPE

Europe possesses the world's oldest, most extensive, and severe data privacy legislation, implemented at national and regional levels. The E.U., through its supranational institutions, has been a pivotal entity in establishing the global paradigm for data protection. Significant E.U. instruments with substantial global ramifications comprise, among others, (a) the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.), 1950 (b) the Convention of the Council of Europe (Convention 108), 1981 (c) the Modernisation of Convention of the Council of Europe (Convention 108+), 2018 (d) Directive 95/46/EC, 1995 and (e) the General Data Protection Regulation, 2018. Firstly, the E.C.H.R., 1950, stands as the foundational convention and a pivotal instrument in the Council of Europe's data protection efforts.[52] The Convention protects various rights, including privacy in personal and family matters. Article 8 affirms explicitly that "every individual has the right to respect for their private and family life, home, and correspondence".[53]

Furthermore, before the 1960s, most international and regional human rights treaties about privacy primarily focused on physical and spatial privacy. Nonetheless, technological advancements during the 1960s and 1970s, especially the enhancement of computer capabilities and their widespread implementation, facilitated the collecting, documenting, organising, and indexing of substantial amounts of personal data. To mitigate such approaches, certain nations have enacted data protection legislation

[50] *Id.* at 457.
[51] *Id.*
[52] E.C.H.R., *supra* note 6.
[53] *Id.* art. 8.

designed to limit information practices. A multitude of interventions differed in scope and execution, resulting in restricted information flows.[54]

3.2.1 DEVELOPMENT OF PRIVACY RIGHTS IN EUROPE

The development of privacy rights in Europe has been shaped by judicial rulings and regulatory frameworks, with the European Union playing a pivotal role in governing personal data usage. This commitment to stringent data control across its fifteen Member States is encapsulated in the Directive 95/46/EC on the Protection of Personal Data, which came into force on October 25, 1998.[55] The Directive encapsulates the concept that privacy is a fundamental human right.[56] The Directive also aims to harmonize data privacy protection standards across E.U. Member States, thereby reducing transaction costs for organisations conducting cross-border operations. It establishes robust personal data protection measures and extends these safeguards internationally by restricting data transfers to third nations,[57] which are classified as nations external to the E.U., unless those countries exhibit a nebulously defined "adequate" standard of data protection.[58]

The European Union regards privacy as a fundamental human right and, accordingly, advocates for stringent protections against the unauthorised commercial exploitation of personal data.[59] European governments have long prioritised identifying the most effective approaches to protect citizens' personal information from misuse; the Directive represents the latest development in this ongoing discourse, which has also unfolded beyond the E.U.'s jurisdiction.

3.2.2 O.C.E.D. PRIVACY GUIDELINES, 1980

In 1980, the Organisation for Economic Cooperation and Development [hereinafter O.E.C.D.] established an international agreement about data privacy.[60] The O.E.C.D.'s rules were designed to address the risk that variations in national laws could obstruct

[54] *See* Mai, *supra* note 24.
[55] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 50.
[56] *See id.* art. 1.
[57] Third Countries refers to Countries outside E.U.
[58] *See* Directive 95/46, art. 25.
[59] *See id.* art 1 (1).
[60] Org. for Econ. Co-operation & Dev. [OECD], Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [hereinafter O.E.C.D. Guidelines] (Sept. 23, 1980).

the unrestricted movement of personal data across borders.[61] The Guidelines outline core principles for safeguarding data privacy, with the O.E.C.D. aiming for these principles to be incorporated into existing national laws or to serve as a foundation for legislation in countries without established data protection frameworks.[62] The principles of the Directive generally adhere to the O.E.C.D. guidelines.

While the O.E.C.D. Guidelines may be endorsed by most countries, the O.E.C.D. lacks the authority to enforce its recommendations and appears either uninterested or unable to address how nations should collaborate to reconcile their varying standards of protection. The O.E.C.D. asserts its commitment to assist member countries in sharing information regarding privacy on global networks and to report on progress towards attaining the objectives of this Declaration. However, it significantly deviates from a definitive commitment to establish a singular international norm.[63]

3.2.3 COUNCIL OF EUROPE CONVENTION 108 (1981)

To strengthen data protection standards, the Council of Europe, which is committed to promoting democracy, human rights, and the rule of law among its Member States, established the Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data.[64] The Convention 108 established essential concepts including data minimisation, purpose limitation, and openness, which were subsequently integrated into the directives and regulations on data privacy.[65] Nevertheless, the Council has predominantly failed to establish standard protection for personal data due to its inability to compel countries to enact legislation under its Convention. Both the O.E.C.D. and the Council of Europe Convention failed to achieve their aims; however, they established the groundwork for the broad and profound protection provided by the directives.[66]

Although the E.U. Data Privacy Directivehas been ratified by the E.U. itself,[67] it is not self-executing. Before adoption in individual Member States, each must establish its legislation. Consequently, it was imperative to harmonize regional data protection

[61] *See id.*
[62] *See id.*
[63] *See* Fromholz, *supra* note 27, at 467.
[64] Council of Eur., Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, C.E.T.S. No. 108 (Jan. 21, 1981).
[65] *Id.*
[66] *See* O.E.C.D. Guidelines, *supra* note 60.
[67] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 50.

mechanisms and policies with national standards. Following years of rigorous efforts and negotiations, the Directives were successfully enacted; nevertheless, the efficacy of this instrument was subsequently undermined by the enactment of the General Data Protection Regulation [hereinafter G.D.P.R.] in 2018.[68]

3.2.4 THE GENERAL DATA PROTECTION REGULATION, 2018

The G.D.P.R.[69] has significantly influenced global data protection rules. The G.D.P.R. serves as a worldwide baseline for data protection regulation, owing to its extensive legal framework, broad extraterritorial applicability, and considerable market impact of the E.U.[70] Consequently, there is a global trend of establishing or updating existing data privacy regulations to align with G.D.P.R. The legal framework, textual nuances, and contextual prominence of G.D.P.R. have attained a pivotal status, making at least a basic understanding of the abbreviation essential for anyone engaged with contemporary discourse.[71]

The G.D.P.R. has supplanted the prior Directive 95/46/EC, introducing significant alterations across various sectors, including technology, advertising, medicine, and finance.[72] It is considered one of the most comprehensive and influential rules, tackling all possible challenges individuals may face about their personal data in the digital age. Post-G.D.P.R., it is claimed that E.U. residents would be informed about the utilisation of personal data by firms and how the E.U. may leverage the advantages of a data-driven economy. Companies often seek clarity to expand their activities securely within the region, and recent data scandals necessitate more precise and rigorous data protection regulations; thus, the E.U. has effectively met its commitments.[73]

[68] *See* Fromholz, *supra* note 27, at 469.

[69] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter G.D.P.R.], 2016 O.J. (L 119) 1.

[70] *See* Marc Langheinrich, *The Golden Age of Privacy?*, IEEE Pervasive Computing, Oct.-Dec. 2018, at 4, 4-8.

[71] *See id.*

[72] *See* Alex Hern, *What is GDPR and How will it affect you?,* The Guardian (May 21, 2018), https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you.

[73] *See* European Commission Statement /18/3889, Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation (May 24, 2018), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889.

3.2.5 ROLE OF EUROPEAN COURTS

The European Court of Justice [hereinafter E.C.J.] and the European Court of Human Rights [hereinafter E.Ct.H.R.] have been instrumental in shaping and broadening the scope of privacy and data protection laws across Europe. The initial lawsuit addressing this topic was *Klass and Others v. Germany*,[74] the Case included covert monitoring tactics employed by the German government for national security purposes. The petitioners contended that these measures infringed upon their privacy rights as stipulated in Article 8 of the E.C.H.R. The Court ruled that covert surveillance is permissible only when it is necessary to safeguard democratic institutions, setting a precedent for balancing state surveillance powers with individual privacy rights.[75]

Subsequently, in the *Google Spain SL* case,[76] the E.C.J. delivered a landmark ruling establishing the "right to be forgotten". In this Case, an individual requested that Google remove outdated and irrelevant information from search engine results. The E.C.J. ruled that individuals have the right to request the deletion of personal data that is no longer relevant. The Court further emphasised the following points: "the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results".[77]

The instances above highlight the growing importance of data protection and privacy rights within the legal framework of the European Union. The E.C.J. and the E.Ct.H.R. have consistently expanded the scope of privacy rights, often due to technological advancements and global issues. This continuous development strengthens the E.U.'s position as a preeminent international data privacy Regulation authority.

4. CROSS-BORDER DATA PROTECTION LAW

In today's increasingly digital world, personal data moves across borders at an unprecedented pace and scale. Global corporations and digital platforms routinely collect, store, and manage data across various countries, making cross-border data flows

[74] Klass and Others v. Ger., App. No. 5029/71, (Sept. 6, 1978), https://hudoc.echr.coe.int/eng?i=001-57510.
[75] *See id.*
[76] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317 (May 13, 2014).
[77] *Id.* ¶ 97.

a crucial component of the modern economy. Personal data has emerged as a valuable raw material, with international data transfer as a key resource for multinational businesses. At the same time, data protection has become a fundamental aspect of the rule of law in the digital age. The disparities in data protection regulations between different jurisdictions now pose a significant challenge to the seamless flow of global data. Balancing the need for unrestricted information exchange with the imperative of robust data protection, irrespective of geographic boundaries, is becoming increasingly essential.[78]

Moreover, cross-border data protection regulation underscores the necessity of ensuring data security following the standards of the originating country when personal data is transferred across national boundaries. The E.U. has consistently led the way in data protection, exemplified by its stringent legislation. However, there remains a lack of consensus among third countries on adopting robust data protection laws. Recently, India has aligned itself with the G.D.P.R. by enacting the Digital Personal Data Protection Act [hereinafter D.P.D.P. Act], which incorporates provisions of the G.D.P.R. that safeguard cross-border data flows. Additionally, the global community must work toward establishing a comprehensive legal framework for cross-border data transfers, ensuring that personal data can move across borders effectively while protecting individuals' rights.[79]

4.1 EUROPEAN LAW ON CROSS-BORDER DATA TRANSFER

The European Union created the G.D.P.R. as a crucial regulatory framework to protect its citizens' privacy and personal information. It has shaped the way many countries and organisations manage personal data and established a global standard for data protection regulations. One of the main characteristics of the G.D.P.R. is its emphasis on transnational data transfers, particularly the transmission of personal data between jurisdictions, including those outside the E.U. Controlling cross-border data transfers is crucial to protecting the security and privacy of personal data in a globalised world where companies and services operate internationally.

Further, regardless of the organisation's location, the G.D.P.R. applies to all organisations that handle personal data belonging to individuals in the E.U. With an emphasis on safeguarding people's privacy and personal information, it provides precise

[78] *See* Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 Eur. J. Int'l L. 441, 441-43 (2010) (U.K.).
[79] *See id.*

protocols for businesses for the gathering, storing, processing, and sharing of personal data.[80]

Key Principles of G.D.P.R. include:

- **Lawfulness, fairness, and transparency:** The Individual shall be kept informed, and data must be processed transparently and lawfully.[81]
- **Purpose limitation**: Personal data must be gathered solely for particular, clearly stated, and lawful purposes.[82]
- **Data minimization**: Only the data necessary for the specific purpose should be processed.[83]
- **Accuracy**: Individual data must be maintained accurately and currently.[84]
- **Storage limitation**: Personal data must not be retained longer than required.[85]
- **Integrity and confidentiality**: Individual data shall be handled in a way that guarantees its security and confidentiality.[86]

4.1.1 CROSS-BORDER DATA TRANSFERS UNDER G.D.P.R.

If specific requirements are fulfilled, including subsequent transfers, the G.D.P.R. permits the transfer of personal data to third nations or international organisations. The G.D.P.R. allows data transfers to nations whose legal systems the European Commission deems to provide an "adequate" degree of personal data protection under the framework of the Directive set forth. Transfers to non-E.U. Nations may take place without such an adequacy judgement under certain conditions, such as the application of binding corporate rules [hereinafter B.C.Rs.] or standard contractual clauses [hereinafter S.C.Cs.]. Under some circumstances, derogations are also permitted. The regulations for cross-border data transfers are outlined in Chapter V (Articles 44–49) of the G.D.P.R., which introduces notable enhancements over earlier Data Protection Directives.[87]

[80] *See* G.D.P.R., *supra* note 69.
[81] *Id.* art. 5 (1) (a).
[82] *Id.* art. 5 (1) (b).
[83] *Id.* art. 5 (1) (c).
[84] *Id.* art. 5 (1) (d).
[85] *Id.* art. 5 (1) (e).
[86] *Id.* art. 5(1) (f).
[87] *See* Shakila Bu-Pasha, *Cross-border Issues Under EU Data Protection Law with Regards to Personal Data Protection*, 26 Info. & Commc'n Tech. L. 213, 222 (2017) (U.K.).

- **Adequacy Decisions: The Gold Standard for Data Transfers**

Article 45 of the G.D.P.R. authorises the European Commission to evaluate whether a foreign country provides an "adequate" level of protection for personal data.[88] This adequacy level requires that the data protection framework of the third country implement measures equivalent to those outlined in the G.D.P.R. The European Commission has thus far issued adequacy conclusions for a select group of nations, namely Japan, Switzerland, Israel, and Canada (on business entities). These judgements enable the effortless movement of personal data without requiring further authorisation, demonstrating the E.U.'s inclination to develop reliable, compatible international partners for data sharing.[89]

Nonetheless, adequacy determinations provide some obstacles. Uncertainty accompanied the post-Brexit adequacy verdict awarded to the United Kingdom. The European Commission's adequacy evaluation of the United Kingdom [hereinafter U.K.] highlighted apprehensions regarding possible divergence in data protection standards following Brexit, especially in light of the U.K.'s intention to promote data flows with nations such as the United States, which lack an adequacy determination under G.D.P.R. criteria. The adequacy mechanism, both as a legal instrument and a diplomatic weapon, reconciles privacy protection with international trade and collaboration.[90]

- **Standard Contractual Clauses and Binding Corporate Rules: Alternatives to Adequacy**

In the absence of an adequacy judgment, the G.D.P.R. provides mechanisms such as S.C.C.s and B.C.R.s, as outlined in Article 46, to legitimise international data transfers. S.C.C.s are legally binding frameworks that organisations can adopt to ensure that third-party data recipients uphold protections comparable to those required by the G.D.P.R. These provisions are essential for businesses transferring data to countries lacking sufficient assessments.[91]

Nonetheless, the *Schrems II*[92] ruling by the Court of Justice of the European Union [hereinafter C.J.E.U.] highlights that applying S.C.C.s alone is insufficient if the recipient country's legal system does not adequately protect personal data. In this landmark ruling, the C.J.E.U. invalidated the E.U.-U.S. Privacy Shield, citing concerns over United

[88] G.D.P.R., *supra* note 69, art. 45.
[89] *See* Kong, *supra* note 78, at 444.
[90] *See id.*
[91] *See id.* at 454.
[92] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd. & Schrems, ECLI:EU:C2020:559, (July 16, 2020).

States [hereinafter U.S.] government surveillance programs that lacked proportionality and judicial redress for E.U. citizens. The Court emphasised that companies using S.C.C.s must evaluate the data protection standards in the receiving country and adopt supplementary measures as necessary, significantly increasing business compliance obligations. The ruling introduced a new standard for implementing S.C.C.s, mandating that companies conduct "case-by-case assessments" to ensure the protection of personal data transferred outside the E.U.[93]

B.C.R.s are intended for multinational organisations that move data internally across international borders. These internal rules require approval from the pertinent Data Protection Authorities and must comply with G.D.P.R. regulations. Although B.C.R.s offer a more adaptable framework for multinational corporations, the protracted and intricate approval process renders them less feasible for small and medium-sized organisations.

- **Derogations for Specific Situations: Last Resort Mechanisms**

Article 49 of the G.D.P.R. outlines specific exceptions that can be used under certain conditions to justify cross-border data transfers in the absence of an adequacy decision or appropriate safeguards, such as S.C.C.s or B.C.R.s. These exceptions include cases where the data subject has explicitly consented, where the transfer is essential for fulfilling a contract, or when it serves substantial public interest considerations. These derogations are carefully defined and intended for limited use, underscoring the G.D.P.R.'s preference for more regulated data transfer mechanisms. This controlled approach to derogations further emphasises the G.D.P.R.'s rigorous framework for protecting personal data internationally.[94]

- **Monetary Fines**

Additionally, Noncompliance with the G.D.P.R.'s regulations governing the transfer of personal data to countries outside the E.U. can lead to substantial fines, marking a significant departure from the penalties under the previous Data Protection Directive. The G.D.P.R. imposes its most severe administrative penalties for breaches of data transfer provisions outlined in Articles 44-49. Organisations found in violation may be subject to fines of up to "4% of their global annual turnover from the preceding financial year or €20 million, whichever amount is greater".[95] The following factors are

[93] *Id.* ¶ 96.
[94] *See* Anna Myers, *Top 10 operational impacts of the GDPR: Part 4- Cross Border data transfers*, IAPP (Jan. 19, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/.
[95] G.D.P.R., *supra* note 69, art. 83 (5).

considered when deciding on a fine: the infringement's kind, severity, and length of time; the act's intentionality; efforts made to lessen the harm it caused; the offender's level of responsibility or relevant history of infractions; the way the infraction was reported to the supervisory authority; adherence to any instructions given to the processor or controller; compliance with a code of conduct; and any other factors that might be considered aggravating or mitigating.[96]

- **The *Schrems I* Case**

Maximillian Schrems, an Austrian, complained to the Irish Data Protection Commissioner in 2013 about Facebook Ireland's transfer of personal data to Facebook's servers in the United States. Schrems contended that his data was not adequately protected by U.S. law, especially given disclosures about surveillance programs such as the Planning Tool for Resource Integration, Synchronization, and Management that gave U.S. intelligence agencies unrestricted access to the personal information of non-U.S. individuals. At the time, the main structure controlling data transmission between the U.S. and the E.U. was the "Safe Harbour" framework.[97] Further, U.S. businesses might self-certify their compliance with European data protection rules under the "Safe Harbour" framework, allowing data transfers from the E.U. without the need for further security measures.[98]

In *Schrems I*, the C.J.E.U. ruled that the "Safe Harbour" agreement was illegal because it was insufficient to protect the personal information of E.U. individuals from arbitrary accessibility by U.S. authorities. The Court emphasised that when transferring data to a non-E.U. countries, E.U. data protection regulations must not be compromised.[99] The Court additionally determined that U.S. monitoring methods infringed against E.U. residents' fundamental right to privacy as stipulated in Article 8 of the Charter of Fundamental Rights and Article 7 of the European Convention on Human Rights.[100] Due to the "Safe Harbour" framework's invalidation, it is currently uncertain whether businesses can legally transfer consumers' personal information from the European Union to the United States.[101]

---

[96] *See id.*

[97] *See* Samuel Gibbs, *What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?*, The Guardian (Oct. 6, 2015), https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

[98] *See* Bu-Pasha, *supra* note 87, at 220.

[99] *See* Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650, (Oct. 6, 2015).

[100] *See id* ¶ 39.

[101] *See id.* ¶ 98.

The *Schrems I* ruling abruptly nullified Safe Harbour, compelling numerous corporations dependent on the framework to urgently seek other data transfer arrangements, including S.C.C.s and B.C.R.s. The European Commission and the United States developed a new framework, known as the E.U.-U.S. Privacy Shield, which was enacted in 2016. Schrems' legal challenges continued, resulting in *Schrems II* and the eventual dissolution of Privacy Shield.

- **The *Schrems II* Case**

Schrems submitted a second complaint with the Irish Data Protection Commissioner after the Privacy Shield framework was implemented, alleging that it was still insufficient to shield E.U. people from American surveillance methods. After that, the matter was heard by the C.J.E.U., which resulted in the landmark *Schrems II* ruling in July 2020.[102]

Further, the Privacy Shield agreement was declared void by the C.J.E.U. in the *Schrems II* case because it did not offer an "adequate" level of protection for the personal information of E.U. persons. The Court concluded that U.S. surveillance statutes, including "Executive Order 12333 and Section 702 of the Foreign Intelligence Surveillance Act", permitted U.S. intelligence services to have extensive access to personal data. Furthermore, E.U. citizens lacked adequate legal recourse to contest such surveillance tactics under the U.S. legal system.[103] The Privacy Shield framework was declared invalid by the Court, but S.C.C.s were upheld as long as businesses took further precautions to secure data that was moved outside of the E.U. The C.J.E.U. stressed that if data exporters are unable to provide a sufficient level of security, they must evaluate the recipient nation's legal system and, if necessary, halt data transfers.[104] The development of cross-border data protection has been significantly influenced by the *Schrems* cases, which highlight the need to provide personal data transmitted outside the E.U. with the same degree of protection as it would inside the E.U. Companies must implement strong data protection procedures when transferring data internationally due to the strict standards set by the C.J.E.U.'s emphasis on the fundamental right to privacy.[105]

[102] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559, (July 16, 2020).
[103] *See id.* ¶ 165.
[104] *See id.* ¶ 26.
[105] *See* Bu-Pasha, *supra* note 87, at 221.

4.2 THE INDIAN LEGAL FRAMEWORK ON CROSS-BORDER DATA PROTECTION

India's regulatory landscape for data protection is evolving, especially regarding cross-border data transfer. As one of the world's largest digital markets, India faces unique challenges balancing the need for stringent data protection with its ambition to establish itself as a global digital leader. The introduction of the Digital Personal Data Protection Act (D.P.D.P. Act), 2023, marks a significant step towards formalising data protection standards, including guidelines on cross-border data transfers.[106] This Section will explore India's current legal framework for data protection, offering a critical analysis of the D.P.D.P. Act, considering the implications of data localization debates, and examining the influence of international law and jurisprudence on India's approach.

India's progress in data protection was initiated with the Information Technology Act, 2000, which laid the foundational legal structure for cybersecurity, data protection, and privacy within the country. An amendment in 2008 introduced Section 43A, imposing liability on corporate entities for inadequate implementation of "reasonable security practices" when managing sensitive personal data.[107] This Regulation, together with the Information Technology Rules, 2011, laid the foundation for privacy protection in India.[108] This method was seen to be limited in its use and lacked the robustness required to address the complexities of modern digital data processing and cross-border data transfers.

With the Supreme Court's landmark decision in *Justice K.S. Puttaswamy,* where the right to privacy was upheld as a fundamental right under Article 21 of the Indian Constitution, the status quo saw a dramatic change.[109] The Court's ruling underscored the critical need for comprehensive data protection laws, leading to the formation of the Justice B.N. Srikrishna Committee. The Committee's report, titled "*A Free and Fair Digital*

---

[106] *See* Anirudh Burman, *Understanding India's New Data Protection Law*, Carnegie India (Oct. 3, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (India).

[107] *See* the Information Technology Act, § 43A , No. 21, Acts of Parliament, (2000), (India).

> **43A. Compensation for failure to protect data:** Where a body corporate, possessing, dealing or handing any sensitive personal data or information in a computer resource which it owns, controls or operates, its negligent in implementing and maintaining reasonable security practices and procedure and therby cause wrongful loss or wrongful gain to any person, such body corporate shall liable to pay damages by way of compensation to the person so affected.

[108] *See* the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, (20110, (India).

[109] *See* Justice K.S. Puttaswamy (Retd.) & Anr, v. Union of India & Ors., (2017) 10 SCC 1 (India).

Economy: Protecting Privacy, Empowering Indians",[110] laid the groundwork for India's inaugural comprehensive data protection legislation, ultimately shaping the D.P.D.P. Act of 2023. The D.P.D.P. Act covers essential facets of data protection, including permission, data localisation, and cross-border data transfers. The Act is less strict than the G.D.P.R.'s comprehensive and rigorous requirements for cross-border data protection, even if it represents significant progress.

4.2.1 CROSS-BORDER DATA TRANSFERS UNDER THE D.P.D.P. ACT

The D.P.D.P. Act, 2023, authorises the transfer of personal data from India to countries specified by the central government, except to jurisdictions which are notified as being restricted, ensuring that the data is protected in a manner comparable to India's domestic standards. This Section mirrors the G.D.P.R.'s adequacy process but is less exhaustive, heavily reliant on governmental discretion. Section 16 of the Act authorises the government to assess foreign jurisdictions for adequacy; however, the criteria for this assessment remain ambiguous.[111] The centralised control of data transfers has raised concerns about the potential influence of political or strategic interests on classifying countries as secure for data transfers.

Additionally, the current version of the D.P.D.P. Act does not provide clear criteria for evaluating the permissibility of data transfers or the process for selecting countries for such transfers. This highlights the need for supplementary frameworks alongside the existing legislation. India could benefit from adopting elements of the European Union's G.D.P.R., which outlines three distinct mechanisms for transferring data outside the E.U. Specifically, Articles 45, 46, and 47 of the G.D.P.R. address "Adequacy Decisions (for pre-approved countries), S.C.C.s, and B.C.R.s, all of which establish frameworks for assessing the legality of cross-border data transfers".[112] The D.P.D.P. Act does not impose a special responsibility on the central government to establish norms of adequacy or other processes for S.C.C.s and B.C.R.s for the regulation or permission of data transfers.[113] As a result, additional compliance measures, reciprocal agreements,

[110] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

[111] *See* the Digital Personal Data Protection Act, § 16 No. 22, Act of Parliament, (2023) (India). Section **16(1): Processing of Personal Data outside India:** The Central Government may by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

[112] G.D.P.R., *supra* note 69, arts. 45, 46, 47.

[113] *See* Anas Baig, *Data Privacy Legislation in focus: A Deep Dive into India's DPDP Act & EU's GDPR*, Securiti (Jan. 24, 2024), https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/.

and conditions, along with contractual provisions, must be put in place to protect the integrity of the crucial data ecosystem.

Moreover, as any critical examination will show, the authority to choose a destination country for data transfer will rest with the Union government. This gives the central government a lot of power in these areas, which could lead to it favouring its own political agendas.[114] In addition, sector-specific regulations might be given priority under the D.P.D.P. Act, as stated in Section 16(2). The D.P.D.P. Act will be superseded by sectors that provide a higher degree of security and set more stringent rules on data flow. Therefore, it's critical to understand that specific industries' expectations make it impossible for certain data types to remain private. However, there is still an unsolved issue with the Act's enforcement and the following penalties, which could make the Act ineffective. As a result, lawmakers must now prioritise the creation of a robust legislative framework to ease the flow of data across borders.[115]

1. **Vague Criteria for Restricting Transfers**: Section 16(1), which talks about processing personal data outside India permits Central Government "by notification" to restrict transfer of personal data to any country or territory outside India, but the Act does not specify what criteria it will use to access whether a destination affords an "adequate" level of protection.[116] This "negative list" methodology assumes permissibility unless explicitly prohibited, reversing the burden seen in G.D.P.R.'s adequacy regime under Article 45, where the European Commission must evaluate objective factors (e.g., rule of law, respect for human rights, data protection rules, onward transfer safeguards) before deeming a country adequate.[117] In the absence of comparable statutory standards, entities encounter ambiguity and possible legal action regarding the circumstances and rationale for restricting transfer.[118]

2. **Centralised Discretion and Risk of Political Influence**: By granting the Union Government sole jurisdiction to enforce limits, the D.P.D.P. Act consolidates significant power at the executive level.[119] Conversely, G.D.P.R. adequacy determinations are made by the autonomous European Commission in conjunction with the E.U. Data Protection

[114] *See* Mahek Sangwan & Sayed Kirdar Husain, *Guarding The Data Frontier: Navigating Cross-Border Data Transfer Under Digital Personal Data Protection Act,* NLR Blog (Oct. 23, 2024), https://nliulawreview.nliu.ac.in/blog/guarding-the-data-frontier-navigating-cross-border-data-transfer-under-digital-personal-data-protection-act/.

[115] *See id.*

[116] *See* Digital Personal Data Protection Act, 2023, § 16.

[117] *See* G.D.P.R., *supra* note 69, art. 45.

[118] *See* Raktima Roy & Gabriela Zanfir-Fortuna, *The Digital Personal Data Protection Act of India, Explained*, Future of Privacy Forum (Aug. 15, 2023), https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.

[119] *See id.*

Board, protecting results from narrow political interests. According to Section 16, the Indian government may block jurisdictions for non-technical or geopolitical reasons without explicit criteria, undermining predictability and hindering legitimate data flows essential for trade, research, and innovation.[120]

3. Sector-Specific Overrides Create Fragmentation: Section 16(2) of the D.P.D.P. Act stipulates that nothing in the Act precludes sector-specific laws (e.g., banking, insurance, telecommunications) from enforcing more stringent cross-border restrictions.[121] This approach honours traditional localisation requirements but also risks creating a fragmented regulatory environment, with financial data governed by Reserve Bank of India regulations, health data regulated by clinical trial protocols, and Aadhaar-linked information according to Unique Identification Authority of India standards. This fragmentation hinders the establishment of a cohesive "one-stop" compliance system and imposes diverse, potentially contradictory obligations on fiduciaries.[122]

4. Absence of an Independent Data Protection Authority: The D.P.D.P. Act establishes the Data Protection Board of India [hereinafter D.P.B.I.] under Section 18 of the Act,[123] and the board has a legislative mandate to function "as an independent body" under Section 28(1) of the Act.[124] Further, the board is the principal entity responsible for enforcing and upholding the legislation. It will function as the principal adjudicative authority, addressing complaints at the beginning. Independence is paramount for the board to administer the law equitably. But the method for appointing the Board members can facilitate its autonomy from the state, draft Rules 16(1), (2), and (3) of the D.P.D.P. Rules, 2025, providing a framework for the Central Government to oversee the Board's nomination process.[125] The Board, as an adjudicatory entity, must consist of individuals nominated by a transparent and dependable independent process, as compared to the G.D.P.R.'s supervisory authority outlined in Article 51.[126] In the absence of a genuinely autonomous regulator empowered to evaluate or veto the Central Government's notifications under Section 16, there exists no internal mechanism to

[120] *See* Baig, *supra* note 113.

[121] Digital Personal Data Protection Act, 2023, § 16. **/longcitation §16(2). Processing of Personal Data outside India: Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary outside India in relation to any personal Data or Data Fiduciary or class thereof.**

[122] *See* Roy & Zanfir-Fortuna, *supra* note 118.

[123] *See* Digital Personal Data Protection Act, 2023, § 18.

[124] *Id.* § 28.

[125] *See* Draft Rules of the Digital Personal Data Protection Act, MEITY, (Jan. 3, 2023), (India).

[126] G.D.P.R., *supra* note 69, art. 51.

monitor discretionary restrictions, nor a platform for fiduciaries to contest politically motivated blocklists.[127]

5. Multinational Corporation Adaptation to D.P.D.P. Act: Multinational corporations operating in India are required to adhere to the D.P.D.P. Act, which mandates obtaining free, informed, and revocable consent for the processing of "sensitive" personal data, safeguarding data subjects' rights to access, correction, and erasure, designating a Data Protection Officer for extensive processing, instituting "appropriate" security measures, and limiting cross-border data transfers.[128] To satisfy these objectives, multinational corporations have undertaken comprehensive data mapping and inventory initiatives to classify Indian personal data by sensitivity and document data flows across global networks, facilitating targeted risk assessments and accurate compliance protocols.[129] They have restructured consent management by substituting bundled or implicit consents with detailed, purpose-specific opt-in processes and streamlined revocation workflows, in alignment with D.P.D.P.'s focus on specificity and purpose limitation.[130] To fulfil the D.P.D.P.'s "reasonable" security requirement as given under Section 8(5) of the Act, Privacy by Design mandates the implementation of Data Protection Impact Assessment, role-based access controls, encryption both at rest and in transit, as well as stringent data minimisation and retention policies.[131] Without an Indian "adequacy" list, Multinational corporations [hereinafter M.N.Cs.] must formulate India-specific Standard Contractual Clauses, solicit preliminary Data Protection Impact Assessment comments, and start a trial Binding Corporate Rules. They also construct "India-edged cloud" architectures to localise data storage and reduce cross-border transfers.[132] Current governance frameworks encompass India-based Data Protection Officers who report directly to senior management, specialised Data Protection and Data Privacy (D.P.D.P.) helpdesks, grievance resolution committees, and the incorporation of D.P.D.P. metrics, such as response times to data subject requests, into global privacy dashboards. MN.Cs. confront practical challenges, including ambiguity regarding "large-scale" processing, postponed

[127] *See* Karthika Rajmohan, *First Read on the Digital Personal Data Protection Rules 2025: Here's what you need to know,* Internet Freedom Foundation (Jan 9, 2025), https://internetfreedom.in/first-read-on-the-dpdp-rules-2025/.

[128] *See* The Digital Personal Data Protection Act,, § 2(l) No. 22, Act of Parliament, (2023), (India). Section 2(l). Definitions: "Data Protection Officer" means an individual appointed by the significant Data Fiduciary under clause (a) of sub-section (2) of section 10.

[129] *See* Deepshikha Sharma, *India's Data Boom and New Thinking About Data Governance,* SCIKIQ (Oct 4, 2024) https://scikiq.com/blog/indias-data-boom-and-new-thinking-about-data-governance/.

[130] *See* Bharvi Shahi & Anand Raj Dev, *Navigating India's Digital Personal Data Protection Act: Critical Implications And Emerging Challenges*, Int'l J. Legal Stud. & Soc. Scis., 2025, at 412, 417 (India).

[131] *See* Ankit Kapoor, *Operationalizing Privacy by Design: An Indian Illustration*, 20 Scripted 5, 11 (2023) (Scot.).

[132] *See* Data Secure, *Impact of the Digital Personal Data Protection (DPDP) Act on Cross - Border Data Transfer,* DPO India, (Mar 5, 2025), https://www.dpo-india.com/Blogs/impact-dpdpa-cross-border/#comparison.

Data Protection Impact Assessment guidelines, and incompatible vendor contracts, by implementing conservative thresholds utilising interim best practices from consulting firms, and renegotiating vendor contracts to incorporate India-specific breach notification timelines and audit rights.[133] To reconcile innovation in Artificial Intelligence/Machine Learning efforts with sensitive data, they generate de-identified datasets and assemble A.I. Ethics Boards to ensure proportionality and necessity. The D.P.D.P. mandates that multinational corporations incorporate an "India Annexe" into their current global privacy frameworks to accommodate India's distinct environment, while the G.D.P.R. offers many lawful bases for processing and a delineated adequacy regime.[134] MN.Cs. should regularly engage with the D.P.B.I. through public comments and meetings, invest in local privacy expertise, automate Data Protection Impact Assessment and consent workflows via Privacy Management Platforms. By understanding the nuances of D.P.D.P., MN.Cs. may mitigate regulatory risks, uphold individual freedoms, and foster innovation within India's rapidly evolving data protection landscape.

5. DATA LOCALISATION AND ITS IMPLICATIONS

Data localisation, or the need that companies store and handle data within the nation's boundaries, has been a contentious issue in India's data protection debates. The Personal Data Protection Bill, 2019, had strict data localisation requirements in previous versions. According to these regulations, sensitive data may only be exported under specific circumstances, while essential personal information must be kept within India. The central government still has the power to restrict some data categories based on national security or strategic interests, even though the final version of the D.P.D.P. Act, 2023, lessens these localisation requirements.[135] The debate about data localisation is fuelled by worries about data sovereignty, safeguarding citizens' privacy from foreign surveillance, and the need for local law enforcement to have quicker access to data. Some people believe that localisation is beneficial to national security. In contrast, others are concerned that it could lead to an increase in operational expenses for multinational

[133] *See* Vinod Mahanta, *Big four firms now grapple with data protection challenges under DPDP Act,* The Economic Times (Oct 6, 2023), https://economictimes.indiatimes.com/news/india/big-four-firms-now-grapple-with-data-protection-challenges-under-dpdp-act/articleshow/104195585.cms?from=mdr.

[134] *See supra* note 130.

[135] *See* Anirudh Burman and Upasana Sharma, *How Would Data Localization Benefit India?*, Carnegie Endowment For International Peace, (Apr 14, 2021), https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india?lang=en.

corporations, a decrease in foreign investment, and the creation of data silos, which would make it more challenging to engage in digital trade across international borders. There are broader worldwide worries about data sovereignty, particularly in rising economies that are attempting to establish greater control over their digital economies, and the debate that is taking place in India is a reflection of these concerns.[136]

6. COMPARATIVE ANALYSIS OF NON-EU ADEQUACY DECISIONS ACROSS KEY JURISDICTIONS.

An analysis of non-E.U. adequacy frameworks uncovers unique approaches by which jurisdictions have conformed to or diverged from the G.D.P.R.'s cross-border transfer regulations, providing useful models for India's developing D.P.D.P. Act.

6.1 JAPAN'S A.P.P.I. AND SUPPLEMENTARY RULES

The Act on the Protection of Personal Information [hereinafter A.P.P.I.] in Japan was initially deemed adequate in 2011 and reaffirmed in 2019, when the Personal Information Protection Commission promulgated binding "Supplementary Rules"[137] that closely align with G.D.P.R. principles, including purpose limitation, data minimisation, and enforceable individual rights, while maintaining flexibility for domestic legal customs (Commission Implementing Decision 2019/419/EU).[138] Japan employs a flexible yet reliable adequacy strategy that harmonises regulatory clarity and procedural agility by integrating statutory amendments and administrative directives.

6.2 UNITED KINGDOM'S POST-BREXIT DATA PROTECTION ACT

Subsequent to Brexit, the U.K. enacted the Data Protection Act 2018, which incorporated the G.D.P.R. into domestic legislation and established the Information Commissioner's Office as an autonomous regulatory body. This mirror-imaging technique supports the

[136] *Id.*

[137] Supplementary Rules means the Personal Information Protection Commission issues binding, detailed guidance (e.g., on cross-border transfer safeguards) that can be updated without fresh legislation.

[138] Commission Implementing Decision (EU) 2019/419 of 23 January 2019, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, 2019 O.J. L (76) 1.

E.U.'s 2016 adequacy decision (Decision 2021/1772/EU), which guarantees seamless data transfers.[139] The U.K. model emphasises the efficacy of statutory isomorphism in maintaining business continuity and illustrates how sufficiency can be enhanced through "sunset clauses" and review mechanisms to accommodate evolving political contexts.

6.3 SOUTH KOREA'S HARMONIZED P.I.P.A.

In 2021, South Korea achieved adequacy by revising its Personal Information Protection Act [hereinafter P.I.P.A.] to include G.D.P.R.-like consent requirements and sanctions while also enhancing the autonomy of its Personal Information Protection Commission (Commission Implementing Decision 2022/254/EU).[140] In contrast to the E.U.'s centralised adequacy reviews, South Korea's framework depends on regular mutual assessments and enforceable guidelines, enabling the nation to adjust standards in response to technological advancements while maintaining treaty-level equivalence.

6.4 ARGENTINA DATA PROTECTION LAW

The Argentine Constitution provides a specific judicial remedy for safeguarding personal data termed "habeas data". This represents a component of the Constitution's framework for protecting constitutional rights, thereby establishing personal data protection as a fundamental right. Argentina received adequacy status (Decision 2003/490/EC) for conforming its legislation to E.U. criteria for data quality, purpose limitation, and legal recourse. It established the Agency for Access to Public Information in 2016 as an autonomous regulatory entity. In contrast to G.D.P.R., which prioritises corporate accountability, Argentina prioritises administrative enforcement and public-sector transparency—an approach that underscores the need for robust institutional design in sustaining adequacy over time.[141]

[139]Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 2021 O.J. L (360) 1.

[140]Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act, 2021 O.J. L (44).

[141]Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, 2003 O.J. L (168).

6.5 COMPARATIVE INSIGHTS FOR INDIA

These jurisdictions exhibit three primary strategies: First, Legal Convergence—alignment of statutes with G.D.P.R. principles; Second, Regulatory Layering—enhancing domestic legislation with obligatory agency regulations; and Third, Institutional Independence—empowering independent supervisory bodies to provide adaptive guidance and perform regular assessments. India's adoption of a G.D.P.R.-inspired adequacy framework, rooted in explicit legislative criteria coupled with Standard Contractual Clauses and Binding Corporate Rules issued by the D.P.B.I., and bolstered by an independent, adequately resourced regulator, would afford multinational corporations both certainty and adaptability in navigating emerging technological and geopolitical challenges.

CONCLUSION

To summarise, a nuanced appraisal of India's D.P.D.P. Act, 2023—when measured against the E.U.'s G.D.P.R.—reveals both promise and peril in India's pursuit of global data integration. The G.D.P.R.'s adequacy regime (art. 45), Standard Contractual Clauses (art. 46), and Binding Corporate Rules (art. 47) embody a transparent, rights-based framework under the stewardship of independent supervisory authorities. By contrast, the D.P.D.P. Act vests undisclosed discretion in the Union Government (sec. 16) to permit or restrict transfers, without publishing objective criteria or timelines. This opacity risks politicization of data flows, especially amid intensifying geopolitical rivalries—for example, India's efforts to balance strategic autonomy vis-à-vis both Western alliances and regional partnerships in the Global South.

Furthermore, India's reticence to embrace G.D.P.R.-style adequacy assessments reflects a trade-off between preserving data sovereignty and unlocking foreign investment, cloud services, and cross-border research collaborations. Sectoral overrides (sec.. 16(2))—from financial data localisation under the R.B.I. to health-data mandates in clinical-trial regulations—compound this fragmentation, burdening organisations with conflicting mandates and leaving enforcement agencies without clear jurisdictional boundaries. In practice, the absence of a genuinely independent Data Protection Board and statutory procedural safeguards (e.g., public consultation, appeal rights) undermines accountability and allows enforcement gaps to persist.

To navigate these challenges, India must pursue a calibrated convergence strategy. This entails articulating statutory adequacy criteria—drawing on G.D.P.R.'s evidence-based assessments—while tailoring them to India's legal traditions and development priorities; promulgating model S.C.Cs. and context-sensitive B.C.Rs. to bridge interim compliance needs; and fortifying the D.P.D.P. Board with clear mandates for impartial oversight, binding timelines, and stakeholder redress. Crucially, such reforms must occur in tandem with diplomatic engagement—for instance, ensuring that any E.U.–India Trade and Technology Council framework factors in India's industrial policy concerns and security imperatives.

In an era where data diplomacy increasingly intersects with national security, economic competitiveness, and human rights, India's regulatory evolution cannot be reduced to mere legislative mimicry. Instead, by embedding transparency, accountability, and principled interoperability into its cross-border transfer regime, India can safeguard citizens' privacy and secure its position as a trusted partner in the global data economy. This balanced approach—grounded in realistic assessments of geopolitical tensions and enforcement capacities—offers the best prospect for reconciling digital innovation, sovereign interests, and fundamental rights on the world stage.

FUNDING STATEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

DECLARATION OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGEMENTS

The authors are grateful to the Faculty of Law, University of Delhi, for facilitating access to library resources that were indispensable to this research. We also thank the two anonymous reviewers for their insightful comments and constructive suggestions, which materially improved the manuscript. Our appreciation goes to the Editorial Board of the University of Bologna Law Review for their professional support and timely correspondence throughout the review process.