Centurion Journal of
Business, Economics and
Social Science
Vol.2 | Issue 1 | June 2025

Outsourcing of Data and Breach of Privacy under Digital Data Protection Act, 2023

Jayprakash Mishra
Assistant Professor, School of Law, Centurion University of Technology and Management, Bhubaneswar, Odisha, India
mishrajayprakash2610@gmail.com
Anuradha Kar
Research Associate, Office of Ld. Advocate General, State of Odisha
anuradhakar97@gmail.com

Abstract

Right to privacy under art 21 of the Indian constitution speaks about the right to life and personal liberty, which has received formal recognition in the case retd. Justice K.S. Puttaswamy v UOI. Major technology giants and social media platforms work on an international level by creating and using data from Indian citizens. This unauthorized use of data creates a grey zone in international law between two countries which has not been addressed in the said act. The digital divide and absence of an international regulatory framework poses a threat to the privacy of data proprietor. The issue of jurisdiction in matters relating to unlawful date trading in cross border is also a matter of concern. The absence of multi-lateral treaties in this regard is also to be discussed.

The goal of the proposed Digital Personal Data Protection Rules is to defend citizens' rights to have their personal information protected. In keeping with India's pledge to provide a strong framework for safeguarding digital personal data, these regulations aim to operationalize the Digital Personal Data Protection Act, 2023 (DPDP Act). In line with the DPDP Act, they aim to uphold the rights of citizens while striking the ideal balance between innovation and regulation, ensuring that everyone may profit from India's expanding

innovation ecosystem and digital economy. They also deal with particular issues including unauthorized commercial data use, digital damages, and breaches of personal data.

Keywords: Right to Privacy, Digital Personal Data Protection Act (DPDP) 2023, Cross-Border Data Jurisdiction, Unauthorized Data Use, International Regulatory Framework

Introduction

There has been a paradigm shift in the way the world revolves. Most of our daily routine revolves around the way we show our life on social media. But it does not preclude us from stressing on the protection of certain data from reaching the public domain or being unauthorizedly used by the "Data privacy presents a confused array of rhetoric and principle. The rhetoric often conflates a wide range of interests and values. Privacy does not neatly fit a single conceptual model".[1] A very large fragment of us stays in the electronic databases. But the contention that stems out of it is that how much do we control the way it is used. This is where the issue of privacy starts. It begins with the way data is generated, how is it preserved and the way it is transferred for the purposes of electronic operations.

The Indian concomitants of privacy are of very recent origin. In the decisions of the Supreme Court in the case of *M.P. Sharma v. Satish Chandra*, the Supreme Court negated the contentions to draw right to privacy, counterpart to the American 4th Amendment rights, into the Indian Constitutional regime.[1] It also held that the state's power of search and seizure has a very strong jurisprudential cover based on the idea of the protection of social security.[1] Further in the case of *Kharak Singh v. State of Punjab*, the Apex Court further held that privacy invasion is not violation of any right under Article 21 of the Indian Constitution[1]. But all the debate came to a halt in the case of *Retd. Justice K.S. Puttuswamy v. Union of India*[1]. In the case, the Apex Court overruled the M.P. Sharma and Kharak Singh judgment. It was of the view that privacy is a basic pre-requisite for exercising liberty and freedom. Privacy thus constitutes basic, irreducible condition necessary for the exercise of 'personal liberty' and freedoms guaranteed by the Constitution. It was held to be a major premise of part III of the Indian Constitution. [1] In many of the following decisions, Supreme Court has held that right to privacy is a fragment of Part III of the Indian Constitution. In the judgment, the Apex Court tried to warn the impeding value of privacy in an information driven society.[1] Three requirements have been established by the Honourable Supreme Court for the State to interfere with fundamental rights. Although the State may step in to defend justifiable state interests, (a) a legislation must exist to support a privacy invasion, as required specifically by Article 21 of the Constitution, (b) the structure and content of the law that imposes the restriction must be within the reasonableness range specified in Article 14, and (c) the methods used by the legislature must be commensurate with the goals and

requirements that the law seeks to satisfy.[1] Therefore, any future legislation that aims to infringe on an individual's right to privacy must pass the proportionality test.

The governing legislation on data protection in India is the Digital data protection Act, 2023. The Act deals with the processing of digital data in such a manner that the right of the individuals to protect their data and the need to process the data for lawful purpose can be governed.[1] The Act being fairly novel in its inception, needs to be discussed in the context of the privacy violations that it seeks to redress. Privacy should be one of the primary concerns of any data protection legislation. The task is to study the interplay of privacy and information in the context of a global information-based society. In the aforementioned judgment, court had commented on the interplay of privacy and informational safeguards in the national context. But most of the information that we used in the way of our dealing in the digital world, involves a cross-border data transfer. The third-party apps that use our data have a global reach which require them to send and receive data in the international sphere. The broad issue for consideration is the issue of privacy violations in cases of data outsourcing under the novel data protection regime.

Literature Review

Data confidentiality, secure query execution, private access, data integrity, and access control enforcement are some of the major issues relating to the outsourcing of data and the privacy issues related therein.[1] It is important to acknowledge the key issues relating to privacy preservation and ensuring execution of encrypted data. There is a conscious argument to reexamine data protection as a separate right from privacy and offers a theoretical framework for proving its inherent worth. The essay by Dr. Tzanou presents a strong argument for reconsidering the legal standing of data protection, contending that it should be seen as a basic right in its own right rather than as a subset of privacy. She identifies the gaps in present legal interpretations and offers a strong framework for bolstering data protection in the EU legal order by critically evaluating current theories and case law. Her study makes a substantial contribution to the current discussion about the best ways to safeguard people's data rights in a society that is becoming more digitally connected.[1] In light of digital surveillance, Nyst and Falchetta's paper examines the development of privacy as a basic human right. It details how privacy is becoming more widely acknowledged in international human rights frameworks, especially in the wake of Edward Snowden's disclosures on widespread surveillance activities. The paper emphasizes how crucial civil society organizations are in establishing privacy standards. Through litigation, especially before the European Court of Human Rights and the Court of Justice of the European Union, advocacy groups have played a crucial role in promoting more robust legal protections and contesting

mass monitoring. The legal challenge against governmental surveillance is one of the article's main themes. The writers look at instances like Schrems v. Data Protection Commissioner and Digital Rights Ireland v. Ireland, which have resulted in important decisions restricting the keeping of large amounts of data. They contend that a large number of national legislations still deviate from international human rights norms, leading to continuous legal disputes.[1] The author talks about the government regulations and the international civil society. But it does not seek to provide any kind of culpability on the private corporations working on the precepts of this data. Further the approach of the author is more of a consumer driven approach and it does not focus on the laches on national security when the data is exchanged between countries by the aforementioned social media giants. Because it enables businesses to access skilled labor across borders, improve efficiency, and minimize costs, offshoring has become a crucial part of global corporate operations. Madhukar, Shivali, and Saini's (2010) paper "Offshoring of Services – An Indian Perspective" offers a thorough analysis of offshore trends, obstacles, and opportunities in India. The paper "Offshoring of Services – An Indian Perspective" offers insightful information about the origins, advantages, difficulties, and prospects of India's offshoring sector.[1] There are still a number of study gaps, nevertheless, especially in the areas of comparative global studies, policy implications, and the impact of developing technologies. To provide a more comprehensive and current understanding of India's involvement in the global offshore scene, future research should concentrate on these topics.

Meaning and Nature of Data Outsourcing

Data outsourcing is the practice of consumers and businesses providing their data, particularly potentially sensitive data, to servers or organizations outside of their control, who subsequently turn into in charge of the data's distribution, administration, and storage.[1] The controller might also keep the information they gather on a third-party cloud platform. As a result, the data controller is no longer in charge of data management.[1] If the data was sent to an external server by a person or another organization, the controller assigns the data to a different business, which is now in charge of data management. The term "data processor" refers to this third-party business.[1] Both the data subject and the collector have no control over the external servers where the outsourced data is kept. Because of processor manipulation, data stored on them could be vulnerable to hacking and leaks.[1] This is troubling since the controller, who was initially given custody of the data, has no authority over the server that houses it. The third-party processor that oversees and controls that server is its property.

Another important type of private wrong arises from unlawful data disclosures. On

several accounts, disclosures have revealed sensitive government information and were also crucial to public policy debate, of which a significant amount of disclosed information is destructive to individuals and companies alike, and often has little, if any, public value. Freedom of expression and privacy are directly at odds when significant disclosures are made to the public and unsettling private intrusions occur. Private information that harms innocent people and businesses is frequently made public when significant information is made public.[1] The harm inflicted on innocent people that is public disclosures emphasize the necessity of striking a balance between people's right to privacy and free speech. A business general counsel sees data breaches as a whirlwind of legal problems. Trademark law, privacy law, insurance law, tort law, negligence, contract law, securities law, violations of foreign data security laws, labour law, violations of federal agency data security, criminal law, shareholder liability, attorney-client privilege, and board liability are some examples of the issues that may arise. It is hard to foresee the precise set of legal problems that will surface following a specific breach, and this list is not all-inclusive[1].

Apart from the organisation level of issues that arise from the data privacy violations, there are certain other forms of sociological level contentions that arise in the same account. In addition to personal harm, "public" or "societal" harm is a second category of privacy wrong. Data privacy, according to academics, is a social ideal and a necessary component of democracy.[1] The parameters of personal information protection are of significant interest to society at large. Protected areas that go against a strictly proprietary, choice paradigm of data privacy is necessary for individual autonomy.

The other important fragment of the data privacy scheme is the public harm arises from offensive and socially corrosive practices. The very specific example of this could be about the allegations on Meta, which is the parent company of Facebook and Instagram, has been called down for civil rights violations. Facebook's parent company Meta has come under fire from civil society organizations for allegedly "whitewashing" a long-awaited assessment on its impact on human rights in India. The paper was released on Thursday in an extremely condensed form. In August 2020, TIME first revealed that Facebook had commissioned the human rights impact assessment (HRIA) to ascertain its involvement in the internet propagation of hate speech. Rights organizations have been waiting for the report for almost two years, as they have long expressed concern that Facebook is causing civil freedoms in India to deteriorate and minorities to face threats.[1]

Further there have been allegation that sometimes data leaks and inefficiency in storing sensitive information have resulted in the violation of certain intellectual

property-based rights and trade secret laws. Individuals' personal information as well as non-personal information like trade secrets, operational data, and commercially sensitive information may be involved in such occurrences. They hurt people by disclosing their personal information, which frequently leads to identity or financial fraud and may jeopardize national and economic security. Additionally, they can seriously disrupt corporate operations or harm a company's reputation, which is more difficult to repair in a setting where customer trust is constantly eroding. These have called a significant loss in the goodwill of the companies. Whenever, there is a leak of data, the competitors have a sweet chance of getting hold of private trade secrets of companies. It is common to hear about cyber security events and breaches of personal data that have a negative effect on thousands of people and businesses. According to a recent survey, there were 59 instances of access sales, 39 ransomware attacks, 107 data leaks, and 388 data breaches. [1]

Data Management regulations under Digital Data Protection Act, 2023

The Digital Data Protection Act, 2023 deals with the protection of digital data in India and provides for remedies in cases of privacy violations. The persons in connection of the Act that hold personal data are called as data fiduciary. Data fiduciary is defined as "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data"[1]. Further significant data fiduciary has also been defined under the Act.[1] There have been numerous allegations that the data fiduciaries used the data for illegitimate uses and for uses not consented by the "data principal"[1]. Misuse of personal information is one of the most significant violations that occur in this regard. This cognizable injury occurs when data is gathered for one reason and then handled differently, failing to uphold the initial expectation.[1] But frequently, this invasion of privacy is overshadowed by the rhetoric around irritation and annoyance. The abuse of personal data that results in the unsolicited solicitation is the fundamental privacy violation. The non-participatory role of the individual in the handling of personal data leads to this misuse. Such an issue arises when participation is solicited under false pretences or when a person is not given the chance to object to the processing of their personal information. Furthermore, data manipulation that goes beyond a person's reasonable expectations is misuse.[1] These all forms of data leaks and privacy violations have to be tackled by the legislations and the judicial precedents that arise in this regard. It is very important to closely look into the statutory and judicial legal framework on the redressal of these violations.

At the very outset, Digital Data Protection Act, talks about the applicability to of the Act to "processing of digital personal data

outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India"[1]. Section 4 talks about the grounds for the processing of personal data. It says that the data can be processed only for lawful purpose and with the consent of the data principal. It further goes on to say that lawful purpose means any purpose not expressly forbidden by law.[1] It proceeds with the requirement of the notice to the effect that the "request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing the data principal about the personal data and the purpose for which the same is proposed to be processed, the manner in which she may exercise her rights and the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed"[1] Further the Data fiduciary is obligated to give the notice to the data principal either in English or in any of the 8 languages mentioned in the 8th Schedule of the Indian Constitution.[1] The consent of the data principal is given sufficient amount of importance by the provisions of the Act. It provides that consent given by the data principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmation action. It further says that an agreement shall be made for the processing of the personal data for the purpose specified and the limitation of the collection of the personal data for that purpose only.[1] But such consent is not irrevocable and can be withdrawn at any time without any technical bars. But the Act further goes on to say that the "consequences of the withdrawal shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal"[1] furthermore, the withdrawing of the consent shall cause the data fiduciary to stop processing the data without reasonable time.

All the aforementioned provisions suffer from some anomalies. Nevertheless, there is no denying that the data gathered has facilitated our lives and contributed to the development of our country. With the aid of all the relevant data that is kept on file on our devices and all of the documents that are nearly connected to one another, the information is at our fingertips. However, it is also undeniable that data mining has encountered problems with self-posts on social media and WhatsApp status updates, among other applications, and that these data extractions—such as address, account details via KYC, phone number, workplace, etc.—have put the individuals to whom they belong at risk.[1]

The definition of the data fiduciary as is mentioned in the Act should be wide enough to cover third parties whom the data fiduciaries generally give the power to deal and process the personal data. Most of

the third parties escape culpability in case of data leaks while taking the defence of third party to the agreement. In law, only the parties to the agreement are bound by it, without making any implication to any third parties. In the case of major data breaches, the third-party data processing companies can take the plea that the data principal has an agreement with the data fiduciary and not the third-party companies and hence cannot implead them in the cases on privacy breach.[1] It is frequently maintained that India ought to switch from the current "consent based" data protection paradigm to a "rights based" one. When the user gives their consent, the data controller can use, process, and share the data with any third parties under the consent-based model.[1] When giving their approval, few people are aware of the true repercussions of the careless data sharing. On the other side, the "rights based" model gives consumers more control over their data while requiring the data controller to make sure those rights are upheld. As a result, users have more control over their personal information. If prior consent from the information provider has been obtained, or if the disclosure is permitted in the contract between the recipient and the information provider, the body corporate receiving the information may disclose sensitive personal data or information to any third party when fulfilling a legal responsibility requires the disclosure.[1] However, in cases where the information is shared with government agencies required by law to obtain information, including sensitive personal data or information for identity verification, or for the purposes of prevention, detection, investigation, including cyber incidents, prosecution, and punishment of offenses, no such consent from the information provider is necessary. There is an imperative requirement to make such third-party access important to be reduces so as to prevent data misuse.

The other significant flaw that remains in this regard is the definition of the phrase “lawful purpose” as used under the provisions of the Act. While some other nations have chosen to include a list of objectives that may be considered "lawful" in their data protection laws in order to lessen the possibility of ambiguity, the phrase "lawful purpose" is still ambiguous.[1] An Act's ease of compliance increases with its level of depth and clarity. It seems that the Act may have grown overly simplistic in its attempt to facilitate company operations while maintaining some level of protection, and as a result, it may prove to be detrimental.

The Digital Personal Data Protection Bill of 2022 established a new idea called "deemed consent," This clause essentially implied that a person's silence or inaction may be interpreted as agreement in certain situations. The deemed consent process has been reframed in Section 7 of the Digital Personal Data Protection Bill (2023) to "certain legitimate uses," which

includes using personal data for the stated purpose, for the State and any of its instrumentalities, and for any of the legitimate uses listed in Section 17. According to section 7 of the DPDP, unless the data principal has expressly objected to the use of the personal data, companies or data fiduciaries may be able to process the data principal's personal data for the purpose for which the data principal voluntarily gave it to the data fiduciary. For instance, All information shared by an employee and all information gathered and processed in connection with his or her immediate employment may be covered by legitimate use if we interpret the provision in the context described above and use the example of a new job. This is because the data is processed for the specific purpose for which the Data Principal voluntarily gave the Data Fiduciary his or her personal information. The Data Principal's approval is not necessary for the company to process the data unless it plans to do so for any other reason than the Data Principal's employment. Since the idea of "certain legitimate use" is still relatively new and unproven, it will be interesting to observe how companies really understand and implement it. While some businesses might be more willing to utilize personal data more widely, others might adopt a more cautious position and solely rely on its permissible usage in extremely specific situations. The courts may also have to decide what "certain legitimate use" means in particular situations, which could help to further define its parameters and how it applies to businesses. But this suffers from various abnormalities that may arise in its application. The definition and the usage of consent may be very free, clear and unambiguous. The consent must not be informed or might be unclear as to its usage. According to the DPDP Bill, organizations who use such consent must be able to demonstrate that it was for "certain legitimate use. People may not be aware that they have given their consent in the first place when it is for legitimate use as defined by the Bill, which makes it challenging for them to exercise their right to withdraw consent. According to the Bill, such consent might not be sufficient for sensitive personal data or children's data, and noncompliance could result in regulatory investigation or legal action. If such consent is questioned, it could be interpreted that the organization has not treated the privacy of data principals seriously, which could harm its reputation.

Regulatory Framework in Data Outsourcing

According to international law's rules of jurisdiction, a state's jurisdiction ends at its borders unless expressly allowed by bilateral or multilateral agreements.[1] However, there are several situations in which the exercise of extraterritorial jurisdiction is permitted by international law.[1] It is simple for personal information belonging to a state's citizens to be processed online across several jurisdictions. This obviously results in a

scenario where a decision made in one state affects or has an influence on another. Processing of data originating from Indian individuals must fall within the purview of extraterritorial jurisdiction.[1]

A client's private and sensitive information assets are frequently transferred across international borders as part of outsourcing agreements. Hospitals, accounting organizations, and insurance companies are entering into contracts with businesses that have facilities abroad. These outsourcers offer services like tax preparation, insurance and medical claim processing, and transcription of doctor's dictation pertaining to every step of the healthcare process, from surgery to patient visits. Most of the time, this data contains private information such social security numbers, medical records, payroll and benefit information, bank records, and purchase history.[1]

In a global economy, offshore outsourcing is still a viable strategic choice.[1] Data security is still the "main deterrent preventing companies (from using) offshore outsourcing. Data sent overseas is only safeguarded to the extent that the provisions of the Contracts stipulate how a cause of action may be enforced and recognized, as permitted by the destination nation. This is challenging because data protection regulations are often unequal outside of the European Union. Therefore, a U.S. corporation's capacity to enforce any data protection clauses in the outsourcing contract is essentially its only option for protecting the personal data it sends to a credit card processing provider in a nation with laxer data protection regulations. In order to reduce their own liability for the outsourcing supplier's conduct, risk-averse businesses are therefore motivated to create insufficient data protection contractual assurances or to omit them completely. It can be difficult to enforce data protection clauses in a foreign sovereign state, even for businesses that are compelled by national legislation to include them in their outsourcing contracts. Bilateral data transfer agreements may help to lessen the enforcement problem, but they cannot be implemented without increasing trade barriers because businesses cannot hire more cost-effective outsourcing providers located in non-participant nations. Globally, there are numerous data protection laws that range from "very strong" to nonexistent. The main issue with offshore outsourcing is when data is moved from a business (or office) that operates in a nation with robust data protection laws. To put it another way, how can one make sure that data protection is not compromised throughout the transfer process when data is moving across borders to a jurisdiction with lax data protection regulations? Technically, data sent overseas may be governed by the laws of the country where it originated, but for jurisdictional and sovereignty concerns, there is no assurance that the data will be protected in the destination country unless

local laws specifically provide for it. The response will change based on whether an intergovernmental standard binds the countries of origin and destination, as well as whether the country of origin has national data protection laws that make businesses that use offshore outsourcing answerable to the public for breaches involving data moved overseas.

Conclusion

There are two methods to guarantee sufficiently robust data protection on both ends of the offshore transaction in the current global regulatory environment: (1) through a contract between the outsourcing company and the outsourced provider; and (2) through bi-lateral agreements on data protection between the outsourced provider's and the outsourcing company's nations. It is currently recommended that businesses looking to outsource "[g]et strong contractual assurances" from the outsourcing provider on data privacy. The outsourcing contract data protection clauses have to outline the business's "control over and access to the data; the use of suitable data security measures; limitations on the use, transport, processing, and sharing of data; a commitment to make modifications as needed by evolving privacy regulations; the right to a facility audit; and numerous other related subjects. The contract must also include a strong enforcement mechanism that makes the BPO provider accountable for fulfilling their end of the bargain. In a country with weak data protection laws (or weak enforcement thereof), it may be necessary for the contract to lay out data protection procedures for the BPO provider. Bilateral cross-border data transfer agreements, like to the U.S.-EU Safe-Harbor agreement, are another way to guarantee robust data protection on both sides of the offshore outsourcing contract. But unless all of these agreements are made, Instead of adopting standardized data protection procedures, this strategy creates a complex network of bilateral treaties with the European Union, meaning that all bi-lateral cross-border data transfer agreements are EU Safe Harbor agreements. Businesses that want to outsource must encourage lawmakers to arrange bilateral agreements between their nation and the outsourcing providers.

Reference

- Kumar, M., Meena, J., Singh, R., & Vardhan, M. (2015). *Data outsourcing: A threat to confidentiality, integrity, and availability.* International Conference on Green Computing and Internet of Things (ICGCIoT), 1496.
- Mills, A. (2004). Rethinking jurisdiction in international law. *British Yearbook of International Law, 84*, 187, 197.
- Mills, J. L., & Harclerode, K. (2017). Privacy, mass intrusion, and the modern data breach. *Florida Law Review, 69*, 771.
- Nyst, C., & Falchetta, T. (2017). The right to privacy in the digital age.

Journal of Human Rights Practice, 1. https://doi.org/10.1093/jhuman/huw026

- Pandozzi, N. R. (2001). Beware of banks bearing gifts: Gramm-Leach-Bliley and the constitutionality of federal financial privacy legislation. *University of Miami Law Review, 55*, 163, 194–197.
- Rai, N. (2020). Right to privacy and data protection in the digital age – Preservation, control and implementation of laws in India. *International Journal of Law and Justice, 11*, 24.
- Rahnama, H., & Pentland, A. (2022, February 25). The new rules of data privacy. *Harvard Business Review*. Retrieved August 1, 2023, from https://hbr.org
- Samarati, P., & De Capitani di Vimercati, S. (2010). Data protection in outsourcing scenarios: Issues and directions. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'10)*.
- Schwartz, P. M. (2000). Internet privacy and the state. *Connecticut Law Review, 32*, 815.
- Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*, 1393.
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*, 1087, 1090.
- Tafti, M. H. A. (2005). Risk factors associated with offshore IT outsourcing. *Industrial Management & Data Systems, 105*(5), 549.
- Tyagi, V. (2013). Legal offshoring industry and data privacy: Global perspectives (with special reference to India). *Indian Journal of Political Sciences, 74*.
- Tzanou, M. (2013). Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right. *International Data Privacy Journal*. Retrieved from https://ssrn.com/abstract=3076415
- West, S. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society, 58*(1), 20.