Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 6 Issue 1 (2026)

Persistent Privacy and Data Security Concerns in the Context of Applicable Laws

Mr. Siddharth Baskar[1], Dr. Vaasawa Sharma[2]

[1]Assistant Professor, School of Law, IILM University, Gurugram
[2]Assistant Professor, School of Law, IILM University, Gurugram

Abstract: In the digital age we are living in now, it is harder to keep data safe and private considering cyberspace continues to grow bigger and there are more cyber threats and data generation. You can get information with just one click. The challenging component is keeping data safe and private for each person. We hear about data breaches every day, which makes us extremely concerned about privacy and data security. The *United Nations International Civil Aviation Organisation* (ICAO) has even investigated claims of a security breach. There are a lot of security challenges that even an established organisation that uses better data privacy and security measures deal with. This makes us question if data protection and security laws are strong enough to reduce cyberattacks. The goal of this research is to analyse the laws that are applicable on data privacy and security. The authors will use a doctrinal research method to examine the case law, statutes, and literature to find flaws in the current system and suggest ways to improve digital security and data protection. The research's goal is to look at how committed countries are to cybersecurity protection on a global scale. The goal is to make people more aware of how important the issue is and how it affects different people.

Keywords: ICAO, Cyberspace, Security Breach, Data Protection, Data Privacy.

1. Introduction

Data protection laws are framed to protect the data which is stored, collected and processed by the organisations or individuals. Every person is entitled to have right to privacy as a fundamental right enshrined in our Constitution under Article 21 (Right to Life and Liberty) and was also laid down in K.S. Puttaswamy case. Till the year 2023, India did not have its own comprehensive and independent legislative framework to protect the data. The foundation was laid down after the advent of Information Technology Act, 2000 which formed a base for the protection of data in India. Indeed, there was a need of a legislative framework which is important for the protection of confidentiality and privacy of an individual's data. In the year 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules) came into existence. Slowly and gradually after the advent of multiple cases and the above case, the process of establishing the comprehensive legislative framework to govern the issues of data protection. After taking various aspects into consideration, the Ministry of Electronics and Information Technology (MeitY), Government of India, set a draft of the Digital Personal Data Protection Bill in 2022 (DPDP Bill). With the passage of time, the draft was passed by both the houses of

the Parliament with some of the changes in the draft on 11 August, 2023 that aims to make an effective regulation in India with regard to data privacy.

There are various compliances including collection, processing, storage and transfer of digital data and its protection which are provided in the DPDP Act. However, more measures on the part of the government are required to make the DPDP Act effective, such as announcing the sections of the DPDP Act itself, abolishing the Privacy Rules, and notifying the rules and regulations essential for effective implementation and enforcement of the DPDP Act. The DPDP Act only applies to personal data in digital form and does not include non-personal or non-digital data. Given this, non-personal data gathering and management are currently uncontrolled in India.

The emerging issue with the DPDP Act is with regard to the applicability of the current law. It is limited to personal data in digital form and does not include non-personal and non-digital data. Given this, non-personal data gathering and management are currently uncontrolled in India. However, the privacy regime in contemporary India is enumerated in the IT Act and Privacy Rules.(Ruiz Ben, E., & Scholl, M. 2023)

Some of the provisions of the DPDP Act are not being implemented yet. Again in the year 2025, MeitY made a draft of DPDP Rules, 2025 for dealing with the public and stakeholders' opinion. The principles of the said act were; firstly, the use of personal data by the organisation is to be done in a lawful, fair and transparent manner secondly, the use of personal data must be limited to such lawful purpose. Only the required information needs to be collected and no more than such limited is necessary. There must be reasonable efforts to maintain the secrecy and confidentiality of the data collected from the individual.

There is undoubtedly, a comprehensive legislation to deal with data frauds and breach but still there are increasing incidences of cyber crimes and data breach in India which includes unauthorised data collection, breach of data, third-party sharing, AI-driven profiling and so on. So, despite of various existing laws, there are many other aspects in which the laws are lagging behind.

As a result, the risk of exposing sensitive information increases which threaten individual autonomy, and can severely damage consumer trust and reputation of the organisations. In cases of unlawful collection of data is increasing rapidly with growing technology. "Around 73% of users believe that their organisations collect their personal data and confidential information without consent and 29% of business leaders stated that their companies use unethical or unauthorised data collection methods, despite being regulatory procedures." (Keller, D. 2018)

1. Security Breach and Data Privacy Laws

The incidences of data scraping are increasing at a high rate. The leaking of personal information is rising especially due to the increase in social networks; the data is available to the public at large. At an average of 534,365 files have the confidential data, which has various entries regarding unlawful data breaches. In the year 2025, the cases of unlawful data collection and the risk has increased gradually.

Information such as names, browsing interests, conversations through the devices and many more are collected unlawfully and without the consent of the owner. In addition to this, the major role is played by the cybercriminals in stealing personal data through various illegal means for example; through using malware, viruses and other illegal applications which the user download without being known of the exact authentic source. (E. Bertino, 2016) In the era of digitalization, data breach has become the most vulnerable incident. Anyone can access the internet anytime, anywhere. Data breach does not only include the personal information such as name, phone number and e-mail, rather it also includes the intellectual property, financial records and any other data which has the content concerning national security.

Such crimes include phishing attacks, trade secrets, hacking etc. The breach of data can occur due to human error also. For instance, if someone clicks on an unauthorised source or link and the site is redirected to a new unsolicited source.

In India, the existing legislative framework is not enough to deal with the issues of data breach because of the gap between legal provisions written in the books of law and the applicability of laws in the modern work. Both are totally different. Undoubtedly, the current legislative framework is strong but lack implementation at the same time. For instance, the DPDP Act, 2023 has been framed and passed to protect the data and curb the cases of data breach but the final rules and procedure is still pending. This results in the exploitation of loopholes by the cyber criminals. The laws on data privacy are made to protect the confidential information but has certain loopholes in it.

The effectiveness of the current legislation is certainly weak. There are gaps in covering the technological advancements like cloud computing, data processing via AI and many more. The issues in ascertaining the jurisdiction is also an issue under the said legislations. Cybercrimes often transcend national boundaries, making prosecution difficult when laws differ between countries. There is an ambiguous definition of data breach and its interpretation is also vague resulting in its weak implementation and clarity. In some cases, the penalties imposed on the accused are very less that it does not leave a deterrent effect on the accused. In addition to this, the agencies responsible for the enforcement of laws lacks the sufficient resources and expertise which may result in low speed of investigations and monitoring. Furthermore, many regulations shift the weight of duty to users rather than making the organisations liable for data protection. These vulnerabilities allow unscrupulous actors and irresponsible organisations to circumvent legal safeguards, jeopardising the intended protections for individual privacy and data security.

2. Impact of Judicial Precedents on Privacy and Data Security

Judicial precedents have affirmed the significance of safeguarding privacy and ensuring data security. The Indian Supreme Court has asserted that the right to privacy is a fundamental right encompassed within Article 21 of the Indian Constitution. (Banerjee, D. 2023).

Let us examine instances of how judicial systems globally have influenced matters:

1. The case of Karmanya Singh Sareen v. Union of India concerned Facebook's acquisition of WhatsApp and its assurance that privacy policies would remain unchanged. In 2016, WhatsApp implemented a new privacy policy permitting data sharing with Facebook. This prompted the petitioners to initiate legal proceedings. In 2021, WhatsApp introduced a new

privacy policy permitting the sharing of data with Facebook, without giving users the option to opt out.

This also resulted in legal issues due to concerns about privacy. The critical enquiries pertained to whether WhatsApp's policy infringed upon the right to privacy, whether Indian users are subjected to disparate treatment compared to European users, and the implications of the mandatory privacy policy under competition law. The Supreme Court of India mandated WhatsApp in 2023 to inform Indian users that adherence to the 2021 privacy policy is not obligatory. (WP (C) No. 7663/2016, Supreme Court of India (2016).

2. In the matter of Google Spain SL v. Agencia Española de Protección de Datos (Mario Gonzalez), a newspaper reported in 1998 that Mr. Mario's property was being auctioned to settle social security debt. In 2009, when Mr. Mario entered his name into Google, he observed that identical information regarding his property appeared in the search results. He subsequently lodged a complaint with the Spanish Data Protection Authority and requested the removal of his information, including links, from Google search results. He also concurred that the initial publication of the newspaper could remain. The Court of Justice of the European Union (CJEU) rendered a landmark ruling establishing the "right to be forgotten." The Court stated that individuals possess the right to remove information and data from search results that is irrelevant, inaccurate, or obsolete. (Case C-131/12, Court of Justice of the European Union).

3. In 2024, the Inter-American Court of Human Rights gave an advisory opinion on Personal Data Protection. This is extremely significant for privacy and data protection. The Court had to decide what the government's duty is when it comes to protecting and regulating data, and whether the American Convention recognises a separate human right to data protection. The Court said that everyone has the right to control their own personal information, which it called the "right to informational self-determination." It also said that this right is essential to human dignity and privacy. The court said that there should be openness about how the data is collected and used, what consent means, and how databases and processing are based on informed consent. The court stated that when it comes to security, protecting personal data must be balanced with freedom of expression and other rights. This advisory opinion has the effect of requiring its members to provide remedies for violations of data rights, raise public awareness, and update legal frameworks. (Advisory Opinion by the Inter-American Court of Human Rights on Personal Data Protection 2024).

4. Prismall v. Google UK ("United Kingdom") Limited and DeepMind – The facts of the case were that the Royal Free UK's NHS Trust ("National Health Services") gave DeepMind Technologies (a Google subsidiary) about 1.6 million medical records in 2015 and 2017. The data that was sent over included private medical records of patients who had been to the Royal Free Trust for tests or hospital stays. DeepMind, a subsidiary of the Royal Free Trust, made an app called Streams that helped doctors find and treat patients. This agreement did, however, let DeepMind use data for business purposes other than direct patient care. Patients did not give their permission for the transfer and use of this data and were not aware that it was being shared.

The High Court had already decided on a "minimum" or baseline claimant and said that a representative suit would probably not be able to prove either a misuse of private information

or a right to compensation for losing control over personal data. The Court of Appeal agreed with this decision. The legal requirement of having the "same interest" was not met because not all members of the proposed class could show a valid, enforceable claim. Because of this failure, the representative action mechanism couldn't be used in this case. The Court pointed out that group claims for misuse of private information are always complicated because different people have different expectations of privacy, which makes it hard to prove that each class member's situation is the same. It also made it clear that this decision does not stop people from making their own claims if their situations support a reasonable expectation of privacy. (2024 EWCA Civ 1516, Court of Appeal UK).

These judicial precedents provide a clear understanding of how judgements have been rendered to safeguard and protect privacy and data.

5. Suggestions

To protect privacy, data protection is extremely important, and quick action is required to do that. Here are some things we believe should be done to protect data and privacy:

1. **Make consent mechanisms more robust**: Sharing data without consent is a violation of privacy. At the moment, we need a well-structured opt-in consent mechanism for collecting and sharing data. This mechanism should also be revalidated on a regular basis to make sure that individuals have given their consent before any such data is collected or shared with a third party. A lot of apps, websites, and services that collect our information don't give us the option to make an informed choice. To improve the process of making informed choices, we need clear privacy notices that explain why data is collected and how it will be used. If we follow these steps, our privacy and data protection will be better. (Walters, R., Trakman, L., & Zeller, B. 2019).

2. **Making granular consent a legal requirement is additionally vital**: This means that users should have more than just a yes or no option for giving their consent for their data to be collected. Granular consent lets users agree to some activities and not others, which protects their privacy. Informed consent, on the other hand, means that users agree to all activities. When India's Digital Personal Data Protection Act (DPDP Act), 2023 goes into effect, it will make informed consent possible, which is also based on the ideas of granular consent. (Gatter, R. 2000).

3. **Data Minimisation**: Privacy policies should require that data be collected only for a specific purpose; otherwise, data sharing and collection should be limited. This would also lower the chance of data breaches and exposure.

4. **China's example**: China sorts data into categories based on how important it is to the country and the public. It also requires data localisation, which means that data created in China must be stored and managed there. For data transfers across borders, the government has to approve them and do security checks. China does not share important data with foreign governments, putting national interests first. We can use their data protection laws as a model to make laws around the world better and stronger. (Yao-Huai, L. 2005).

5. Conclusion

Data security and privacy are closely linked, and it's important to know how to protect this data. More international conferences and better policies are needed to better understand the subtleties of technology and the security issues that come with it. It's time to do something now to make things better in the future. Data is sensitive, and if we don't handle it correctly, it could lead to breaches and, in the end, violations of privacy. The courts need to be very important in making rules and helping the legislature add the necessary laws to protect and enforce data stabilisation.

7. References

1. Advisory opinion issued in 2024 by the Inter-American Court of Human Rights on Personal Data Protection.
2. Banerjee, D. (2023). The K. S. Puttaswamy judgement and its pivotal role in reproductive rights. SSRN Electronic Journal, 20–30. https://doi.org/10.2139/ssrn.4322166
3. Bertino, E. (2016). Data security and privacy: Concepts, approaches, and research directions. In 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) (pp. 400–407). IEEE. https://doi.org/10.1109/COMPSAC.2016.89
4. Court of Appeal judgment on Prismall v Google UK Ltd and DeepMind Technologies Ltd, 2024.
5. Documentation from Karmanya Singh Sareen v. Union of India, Supreme Court of India, accessed through legal case commentary and court documents.
6. Gatter, R. (2000). Informed consent law and the forgotten duty of physician inquiry. PubMed, 31(4), 557–597. https://pubmed.ncbi.nlm.nih.gov/11962530.
7. Judgment in Google Spain SL v. Agencia Española de Protección de Datos, CJEU, 2014.
8. Keller, D. (2018). Comments on the guidelines on transparency under Regulation 2016/679. SSRN. https://ssrn.com/abstract=3262947.
9. Ruiz Ben, E., & Scholl, M. (2023). Methods for implementing usable secure online public services. In Usable Privacy and Security in Online Public Services (pp. 59–87). Springer Nature Switzerland.
10. Walters, R., Trakman, L., & Zeller, B. (2019). Data protection law: A comparative analysis of Asia-Pacific and European approaches. Springer Nature.