The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

EXPLORING THE INTERSECTION OF TECHNOLOGY AND PRIVACY LAWS IN INDIA

INTRODUCTION

As technology rapidly advances and becomes more affordable and accessible, the threat to individual privacy grows. With the advancement in information technology, there is a growing concern as personal data becomes more accessible, reducing individual's control and potentially leading to various adverse consequences.

Privacy is the freedom to be left alone without any intrusion. Just as individuals enjoy spending time alone as much as socializing, any violation of their privacy evokes a strong sense of discontent. Similarly, when it comes to personal data privacy, its invasion can create hindrances in an individual's life, ranging from financial theft to exposure of private information stored in their phone.

India recognizes the significance of balancing technological advancements with individual privacy rights. This article talks about the Various laws and regulations that are in place to ensure responsible handling of personal information in digital realms.

THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act of 2000 was enacted during a budget session of parliament. It was signed by President K.R. Narayanan in 2000, and was further refined by India's Minister of Information Technology, Pramod Mahajan.

The original IT Act of 2000 focused on electronic documents, e-signatures, and penalties for security breaches like cyber terrorism. Regulating authorities were empowered to monitor and create rules for such situations. As technology evolved, the act was updated in 2008 to include mobile devices as "communication devices" and hold IP address owners accountable for

accessed content. In 2011, privacy measures were strengthened, imposing strict requirements on collecting personal information

Offences under the Information Technology Act, 2000

The Information Technology Act, 2000[1] specifies various offenses such as Tampering with computer source documents, Hacking computer system, Publishing offensive, false or threatening information, Receiving stolen computer or communication device, cheating using computer resource, using password of another person, acts of cyber terrorism, publishing information which is obscene in electronic form, publishing private images of others, publishing images containing sexual acts, publishing child porn or predating children online, etc. These offenses carry severe penalties, including imprisonment and/or fines ranging from ₹100,000 to ₹1,000,000.

In the case of Avnish Bajaj v. State (N.C.T.) of Delhi[2] a student named Ravi Raj, posted an obscene MMS video for sale on baazee.com. Avnish Bajaj, CEO of the website, was accused. The issue was whether the website is liable for the content and if Avnish Bajaj should be held responsible.

The court found a prima facie case against the website for listing and the video under IPC Sections 292(2)(a) and 292(2)(d). Even though the website had a filter to prevent such content, Ravi Raj still managed to post it with a description mentioning “DPS Girls having fun.” Avnish Bajaj, however, was discharged under IPC Sections 292 and 294 as the law doesn't automatically hold a director criminally liable if the company is accused. For the IT Act, Avnish Bajaj faced a prima facie case under Section 67. Despite not being declared guilty, conditions for bail included surrendering his passport and not leaving India without court permission.

Amendments to the Information Technology Act in 2008 enhanced the original legislation by updating and clarifying terms. It broadened the definition of cybercrimes and validated electronic signatures. The Act is applicable to individuals, companies, or organizations using computer resources, comprising nine chapters and 117 sections.

The Information Technology Rules of 2011 focus on safeguarding personal data collected by individuals or those engaged in commercial or professional activities. Key changes involve

[1] THE INFORMATION TECHNOLOGY ACT, 2000, § 66,66A,66B,66C,66D,66E.66F,67,67A,67B, No. 21, Acts of Parliament, 2000 (India)
[2] Avinish Bajaj v. State (N.C.T.) of Delhi, (2008) 105 DRJ 721: (2008) 150 DLT 769.

rules for regulating intermediaries, imposing fees for cybercrime violations, addressing cheating, and setting other restrictions.[3]

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

On August 11, 2023, the President of India approved the Digital Personal Data Protection Act, 2023 (DPDP Act), which focuses on safeguarding digital personal data in the country. The Act applies to data collected digitally or converted from non-digital sources.

Under this act before using personal data, companies must get permission, except in specific situations outlined in the law. Companies also must create ways for users to raise concerns, and there's a board (Designated Professional Body) to handle complaints and penalize those not following the rules. People have the right to access, correct, update, and delete their data. They can also nominate someone to manage their data rights. There are special rules to safeguard children's data, requiring extra care and consent. Businesses must clearly state why they collect data and ensure its security. They also need to set up systems to address people's complaints.[4]

Section 2(t) of the Digital Personal Data Protection Act, 2023 defines “personal data” as any data about an individual who is identifiable by or in relation to such data. Section 2(u) defines "personal data breach" as any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.[5]

KEY POINTS OF THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023 requires Indian enterprises to make fundamental changes in how they handle privacy and personal data. It reflects India's unique approach to personal data protection, addressing the challenges posed by increasing internet usage. Here are some key highlights of the act.

- Consent and Legitimate Use:

Companies can only handle digital personal data with the consent of the individual. It is called as the data principle. The Consent must be obtained even if it was given previously. If consent

[3] THE LEGAL QUORUM, https://thelegalquorum.com/online-privacy-and-cybersecurity-challenges-and-regulations/ (last visited March 02, 2024)
[4] CARNEGIE INDIA, https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624#:~:text=The%202023%20act%20creates%2C%20for,clearly%20enumerated%20in%20the%20law (last visited Feb 28, 2024)
[5] DIGITAL PERSONAL DATA PROTECTION ACT, 2023, § 2(t), 2(u), No. 21, Acts of Parliament, 2023 (India)

for processing digital personal data is withdrawn, companies must promptly cease the data processing activities.

- Data Protection Beyond India's Borders

The DPDP Act is relevant to any data, whether it was originally in digital or physical form and later converted to digital in India. It also applies to the handling of digital personal data even if it goes beyond India's borders, especially when providing goods or services to people within India.

- Data Protection Board

The Data Protection Board acts as an impartial body to resolve privacy-related disputes. As an independent regulator, it has the power to identify non-compliance with the Act and impose penalties. The central government appoints the chief executive and board members, ensuring a fair selection process. An appellate body will be established to allow customers to challenge decisions made by the Data Protection Board, possibly assigned to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).[6]

- Breach Reporting

Personal data breaches must be reported to affected individuals and the Data Protection Board of India. A breach includes unauthorized processing, disclosure, use, alteration, or loss of personal data affecting its confidentiality, integrity, or availability.

- Significant Data Fiduciaries

Entities handling substantial personal data may be designated as "Significant data fiduciaries."

These entities must meet additional standards, including engaging an independent data auditor to check and ensure that they are handling the personal data responsibly and securely and also need to regularly assess and document the potential risks and impact of how they collect, store, and use personal data. This helps in identifying and addressing any potential privacy concerns.

- Data Ownership Rights

Individuals have rights, including access, rectification or deletion, filing grievances with the data fiduciary, and the ability to appoint someone to exercise these rights on their behalf.

---

[6] INDIA BRIEFING, https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/ (last visited Feb 29, 2024)

- Limitations on Data storage

Section 8 of the DPDP Act emphasizes that data fiduciaries must delete information when consent is withdrawn or when the data is no longer serving its original purpose. The collected data is not stored indefinitely. It should be kept for the minimum required time and disposed of safely when no longer needed.

- Penalties

The act outlines penalties for different violations, including fines of up to Rs 250 crore for neglecting security measures to prevent data breaches and up to 200 crore for failing to fulfil obligations regarding children's data. The Board will determine these penalties following an inquiry. An individual whose data is processed (Data Principles) must also refrain from registering false or frivolous complaints, providing incorrect information, or pretending to be someone else in specific cases. Breaching these duties may result in a penalty of up to Rs 10,000.[7]

The DPDP Act reflects India's unique approach to personal data protection, addressing the challenges posed by increasing internet usage and cross-border trade. While not as detailed as some international standards, the Act requires Indian enterprises to make fundamental changes in how they handle privacy and personal data.

NATIONAL CYBER SECURITY POLICY, 2013

Cybersecurity is like a digital guardian that protects our online world from malicious activities. It involves safeguarding digital devices like computers, servers, mobiles, electronic systems, networks, and data from harmful attacks. As our world becomes more interconnected and data-driven, cybersecurity plays a crucial role.

In 2013, the National Cyber Security Policy was introduced to monitor, protect, and enhance defences against cyberattacks. This policy aims to ensure a secure cyberspace for individuals, organizations, and the government. It focuses on safeguarding information infrastructure, reducing vulnerabilities, developing capabilities to prevent and respond to cyber threats, and minimizing damage from cyber incidents.[8] The policy also aims to protect important

[7] PRS LEGISLATIVE RESEARCH, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#:~:text=Data%20principals%20will%20have%20certain,of%20up%20to%20Rs%2010%2C000. (last visited March 02, 2024)

[8] GEEKS FOR GEEKS, https://www.geeksforgeeks.org/the-national-cyber-security-policy-2013/ (last visited, March 03, 2024)

information like personal details of people using the internet, banking info, and our country's important data.

NEED FOR THE NATIONAL CYBER SECURITY POLICY, 2013

With rising cyber threats, it's vital to prioritize cybersecurity. The 2013 National Cyber Security Policy focuses on safeguarding information and curb the growing misuse of technology. Its need arises for various several reasons.

- Developing processes to analyze and manage information handling, and build capabilities to prevent and recover from cyber incidents, making the online environment stable and resilient and to ensure people can safely use the internet for everyday activities while protecting their rights like freedom of speech and privacy.
- Creating better and stronger rules and laws to prevent cybercrime.
- Strengthening collaboration between institutions, organizations, and companies at national and international levels to build trust and collectively address cybersecurity risks and promote cooperation between public and private sectors for cybersecurity by jointly developing strategies and sharing threat intelligence.
- Improving the capabilities of cybersecurity professionals to effectively counter online threats. Also, educate and make the public more aware of potential risks and how to stay safe online.
- Collaborating with other countries to share knowledge, resources, and strategies for tackling global cybersecurity challenges. This international partnership helps create a more secure cyberspace for everyone.

NATIONAL CYBER SECURITY STRATEGY 2023

The National Cyber Security Reference Framework (NCRF) 2023 has been approved and will be placed in public domain. The national cyber security coordinator Lt Gen (Retd) Rajesh Pant, said the NCRF policy will be aimed at helping critical sectors such as banking, energy and others with a “strategic guidance" to address cyber security concerns. Further he stated that National Cyber Security Strategy 2023 is an important document that supersedes the 2013 policy. From 2013 till 2023, the world has changed as new threats have emerged calling for new strategy. Organizations can utilize the NCRF to enhance their cyber defences, mitigate data breach risks, ensure regulatory compliance, and improve operational efficiency. The government has invested ₹700 crore in a national cyber awareness and skilling initiative. The

document will be put in public domain after a final check by the committee to ensure that nothing confidential is released.[9]

RIGHT TO PRIVACY

A nine-judge Constitution Bench headed by Chief Justice, J.S. Khehar on 24th August, 2017 gave a landmark decision on Right to Privacy. The Supreme Court ruled that Right to Privacy is "intrinsic to life and personal liberty" and is inherently protected under Article 21 and as a part of the freedoms guaranteed by Part III of the Indian Constitution.[10]

The Supreme Court has integrated privacy into the core of our rights and freedoms by considering it an inherent part of life and liberty under Article 21. This means that anyone, regardless of nationality, can seek legal recourse through articles 32 and 226 of the Indian constitution if their privacy is violated.

The court has emphasized that privacy is a crucial element of various fundamental freedoms outlined in Part III of the Constitution. These freedoms include the right to equality, free speech, expression, religion, and other essential rights needed for a dignified life. However, these rights are subject to reasonable restrictions for public health, morality, and order.

In the famous telephone tapping case of People's Union for Civil Liberties v. Union of India[11] where the petitioners challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885 which empowered the Central or State government or its authorised officer to intercept and record messages in case of public emergency or in public interest.

The court held that only high-ranking government officials could carry out such interceptions, and only when absolutely necessary, for a limited period of six months. Furthermore, it emphasized that once the messages were no longer needed, they must be promptly deleted. Recognizing a person's Right to Privacy, it ordered the formation of a Review Committee to check that such interception was not in contravention of Section 5(2) and if it was, the messages shall be destroyed immediately.

CONCLUSION

[9] HINDUSTAN TIMES, https://www.hindustantimes.com/cities/pune-news/national-cyber-security-strategy-2023-to-be-released-soon-101686596627065.html (last visited, 05 March, 2024)
[10] Justice K.S. Puttaswamy and Anr. v. Union of India and Ors., (2017) 10 SCC 1, AIR 2017 SC 4161.
[11] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

In the rapidly evolving world of technology, the need to protect personal privacy has become more crucial than ever. India has addressed this challenge by enacting laws to safeguard digital information. The Information Technology Act of 2000, with subsequent amendments, has laid the foundation for addressing cybercrimes, while the Digital Personal Data Protection Act of 2023 reflects India's unique approach to personal data protection in the face of increasing internet usage.

The National Cyber Security Policy of 2013, and the subsequent National Cyber Security Strategy of 2023, demonstrate India's commitment to creating a secure cyberspace by monitoring, protecting, and enhancing defences against cyber threats. These policies emphasize collaboration between institutions, organizations, and countries to collectively address cybersecurity risks and promote public-private partnerships for a safer online environment.

However, despite these measures, cybercrimes are on the rise. Recently, there have been cases where people were tricked into transferring large sums of money over the phone. The scammers use various tactics and even provide fake evidence to make their scheme seem legitimate. When asked for their name or ID, they quickly disconnect the call.

India has taken important steps to protect the privacy in digital age. Laws and rules have been set up to make sure our personal information stays safe. But the world of technology is always evolving, and we need to keep up. The responsibility doesn't solely lie with the government; individuals, in particular, need to be vigilant when sharing private information online, over the phone, or during video calls to ensure online safety. It's a team effort to face the challenges that keep popping up in our digital world. By staying alert, working together, and taking proactive steps, we can find the right balance between technological advancements and the protection of individual privacy rights.