

The Lack of Pro - Privacy Legislations in India and the Growing Threat of Identity Theft: A brief Introduction

Soumyadeep Chakrabarti

Assistant Professor, Faculty of Law, Kalinga University, Naya Raipur, India

How to cite this article: Soumyadeep Chakrabarti (2024). The Lack of Pro - Privacy Legislations in India and the Growing Threat of Identity Theft: A brief Introduction. *Library Progress International*, 44(3), ----.

Introduction:

In the digital age, privacy and data security have emerged as critical concerns for individuals, organizations, and governments worldwide. In India, the lack of comprehensive privacy laws and the easy access to government-issued ID cards by online criminals present significant challenges. These issues are compounded by the Indian government's efforts to monitor its citizens through various legal frameworks, highlighting the urgent need for an ombudsman or consumer court to address these concerns and provide speedy justice.

The Current State of Privacy Laws in India

India's legal framework for privacy is fragmented and lacks a unified approach. The Constitution of India, under Article 21, guarantees the right to privacy as a fundamental right. This was reinforced by the landmark judgment in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹, where the Supreme Court of India affirmed that privacy is intrinsic to life and personal liberty. However, the implementation of privacy rights in India is far from comprehensive. The primary legislation governing data protection is the Information Technology Act, 2000 (hereinafter referred as the IT Act), and its subsequent amendments. The IT Act includes provisions related to cybercrimes and electronic commerce but does not adequately address issues of personal data protection and privacy.

Lack of a Comprehensive Data Protection Law

The Digital Personal Data Protection Act, 2023, was introduced to address these gaps, aiming to create a framework for the protection of personal data and establish a Data Protection Authority of India. However, the bill in its infancy has faced criticism for its various provisions, including broad exemptions for government agencies, which undermine the very purpose of protecting personal data.

The Threat of Identity Theft

Identity theft has become a pervasive issue in India, with online criminals exploiting the easy access to government-issued ID cards such as AADHAAR, PAN cards, and driving licenses. These documents are often required for various services and transactions, both online and offline, making them prime targets for fraudsters.

Case Study: The AADHAAR card data leak case

AADHAAR, the world's largest biometric ID system, has been at the centre of numerous controversies regarding data privacy. In 2018, a report by 'The Tribune' revealed that personal information of millions of AADHAAR holders was available for sale on the internet for a mere ₹500. This breach exposed sensitive data, including names, addresses, phone numbers, and AADHAAR numbers, highlighting the vulnerabilities in the system.

Supreme Court Rulings on AADHAAR

The Supreme Court of India, in its judgement in the case of *K.S. Puttaswamy v. Union of India*², upheld the

¹ (2017) 10 SCC 1.

² (2017) 10 SCC 1.

constitutionality of the AADHAAR scheme but imposed several restrictions on its use to protect privacy. The court ruled that AADHAAR could not be made mandatory for services such as bank accounts and mobile connections, although it remained compulsory for PAN cards and income tax returns.

Government Surveillance and Privacy Concerns

While the threat of identity theft looms large, the Indian government's initiatives to monitor its citizens also raise significant privacy concerns. Various laws and policies have been introduced to enhance surveillance capabilities, often at the cost of individual privacy.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules impose stringent requirements on social media intermediaries and digital platforms to monitor and regulate content. Critics argue that these regulations infringe upon freedom of expression and privacy rights by enabling government surveillance.

The Communication Surveillance Laws

India's surveillance framework includes laws such as the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. These laws grant the government broad powers to intercept and monitor communications, often without adequate judicial oversight.

Case Study: Pegasus Spyware Controversy

In 2021, it was revealed that the Pegasus spyware, developed by the Israeli company NSO Group, had been used to target journalists, activists, and politicians in India. This scandal underscored the extent of surveillance and the lack of accountability in the use of such technologies.

The Need for an Ombudsman or Consumer Court like Adjudication

Given the dual threats of identity theft and government surveillance, there is an urgent need for a dedicated mechanism to address privacy violations and provide swift justice. An ombudsman or consumer court specifically for privacy and data protection issues could serve this purpose effectively.

Role and Functions of the Ombudsman

An ombudsman for privacy could act as an independent authority to oversee and investigate complaints related to data breaches, identity theft, and unauthorized surveillance. The ombudsman would have the power to enforce compliance with privacy laws, order compensation for victims, and impose penalties on violators.

Fast-Track Consumer Courts like Adjudication

Consumer courts like structures which will be dedicated to privacy issues could expedite the resolution of cases, ensuring that victims of identity theft and data breaches receive timely justice. These courts could handle cases involving financial fraud, misuse of personal data, and violations of privacy rights, providing a streamlined process for redressal.

Case Law and Supreme Court Judgements

Several Supreme Court judgements have addressed issues related to privacy, data protection, and government surveillance, setting important precedents.

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)³

As mentioned earlier, this landmark judgement recognized the right to privacy as a fundamental right under the Indian Constitution. The court emphasized that privacy encompasses personal autonomy, including the right to control personal information. This judgement on the AADHAAR scheme addressed privacy concerns and set limits on the mandatory use of AADHAAR for various services. The court ruled that AADHAAR could not be made mandatory for services such as bank accounts and mobile connections.

2. Shreya Singhal v. Union of India (2015)⁴

In this case, the Supreme Court struck down Section 66A of the Information Technology Act, which criminalized offensive online content. The court held that the provision was vague and violated the right to free

³ (2017) 10 SCC 1.

⁴ AIR 2015 SC 1532.

speech and expression under Article 19(1)(a) of the Constitution.

3. Anuradha Bhasin v. Union of India (2020)⁵

In this case, the Supreme Court addressed the issue of internet shutdowns in Jammu and Kashmir. The court held that indefinite internet shutdowns violate the right to freedom of speech and expression and the right to carry on business, and that such orders must be temporary, limited in scope, and justified.

Conclusion

The lack of comprehensive privacy laws in India, coupled with the easy access to government ID cards by online criminals, poses significant risks to individuals' privacy and security. At the same time, the government's efforts to monitor its citizens through various laws highlight the need for a balanced approach that protects privacy while ensuring national security. Establishing an ombudsman or consumer court for privacy issues could provide a much-needed mechanism for addressing these concerns and delivering speedy justice. By learning from the experiences of other countries and implementing robust data protection frameworks, India can safeguard its citizens' privacy and build trust in the digital age.

References

1. Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) - Supreme Court of India
2. Justice K.S. Puttaswamy vs Union of India (2018) - Supreme Court of India
3. Shreya Singhal vs Union of India (2015) - Supreme Court of India
4. Anuradha Bhasin vs Union of India (2020) - Supreme Court of India
5. Information Technology Act, 2000
6. Personal Data Protection Bill, 2019
7. The Tribune report on AADHAAR data breach (2018)
8. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
9. Indian Telegraph Act, 1885

⁵ AIR 2020 SC 1308.