CORPORATE LIABILITY FOR DATA BREACHES IN INDIA: LEGAL FRAMEWORK, CHALLENGES AND IMPLICATIONS

- Manisha Debnath*

Abstract

In today's digital world, companies collect, store and manage large amounts of user's personal data. They are also vulnerable to data breaches. This type of incident not only harms companies' reputations but also leads to legal and financial consequences. This article explores the legal accountability of corporations in data breach cases, and it also focuses on major regulations such as GDPR, CCPA, and India's DPDP Act of 2023. It explores real-world case studies and legal consequences and penalties. The article highlights the legal impact of breaches and suggests practical strategies for companies to improve their data security and ensure compliance.

Keywords: *Data, Breach, Legal Framework, Cybersecurity, Criminal Liability, Civil Liability.*

* LL.M. Student @ ICFAI University, Dehradun

INTRODUCTION

A data breach occurs when private or sensitive information is accessed by an unauthorized individual. Data breaches have become increasingly frequent since corporations and the government switched from paper to digital storage. A data breach may have serious financial repercussions for businesses, including direct expenses like fines and indirect ones like damaged brand reputation and lost customer trust. Data breaches may be caused by a variety of methods, including malware, phishing, hacking, etc. Sensitive data include financial information like credit card numbers and bank account numbers, protected health information like medical records and personal information, and identifiable information like name, address, date of birth, and social security number. The sectors and the particulars of the breach frequently determine the kind of private information that is targeted. According to a report by the think tank Data Security Council of India (DSCI), India saw an average of 761 cyberattack attempts every minute in 2024, with the healthcare sector being the most common target, followed by the hotel and banking industries.[1]

OBJECT OF THE RESEARCH ARTICLE

1. To compare India's practices with other global practices for data breaches and
2. To study how effective the Indian data protection law is in preventing data breaches.

LEGAL FRAMEWORK AND REGULATIONS

General Data Protection Regulation (GDPR)

GDPR is the world's strictest law when it comes to privacy and security. The GDPR was drafted and adopted by the European Union. On May 25, 2018, marked the implementation of the GDPR. The GDPR applies to all businesses, regardless of their location, any businesses that handle and process the personal information of individuals residing in the European Union. Certain types of data are recognised under GDPR, such as ethical and political views, biometrics, etc. Users are granted rights under the GDPR, such as accessing personal data, deleting, restricting, porting data, and objecting to automated data processing. Before collecting data and setting cookies on the user's device, websites must obtain their consent.

[1] Aakash Sharma and Jainam Shah, "2024: A Year of Data Leaks, Espionage, and DDoS Attacks," *India Today; available at*: https://www.indiatoday.in/india/story/2024-a-year-of-data-leaks-espionage-and-ddos-attacks-ransomware-data-breach-2654230-2024-12-23 (last visited on: 10.04.2025)

General Data Protection Regulation carries seven principles to safeguard user privacy and security:

1) *Lawfulness, fairness and transparency*: data processing must adhere to these standards,
2) *Purpose limitation*: the reason for processing the data must be valid,
3) *Data minimisation*: data will only be collected or processed as much as necessary,
4) *Accuracy*: the information gathered must be up to date and correct,
5) *Storage restriction*: the amount of personal information required for the intended use shall be kept on file,
6) *Integrity and secrecy*: processing must be done in a way that ensures sufficient security, integrity, and confidentiality; *for example* - encryption may be used, and
7) *Accountability*: the data controller is accountable for proving compliance with all of these GDPR principles.

GDPR guidelines for processing personal data

1) The user's consent must be sought before processing any data,
2) Processing is necessary to fulfil or be ready for a contract involving the data subject,
3) Processing is necessary for you to fulfil a legal obligation,
4) The data must be processed in order to save a life,
5) Processing is necessary to carry out an official responsibility or a job of public interest, and
6) You have a valid reason to process someone's personal data. This is the most adaptable legal basis, but the *"fundamental rights and freedoms of the data subject"* always take precedence over your interest, particularly when it involves a child's data.

GDPR facilitates two categories of measures that are made possible: technical measures and organisational measures. In technical measures, employees are advised to sign end-to-end encryption contracts with cloud providers or use two-factor authentication. Organisational measures include training workers, establishing a data privacy policy, and restricting access to personal data to only those employees who require it.

GDPR sanctions for non-compliance businesses who break the GDPR rules may be fined up to €20 million, or 4% of their yearly worldwide turnover. This is the highest penalty that may

be imposed for the most serious violations, such as processing data without sufficient customer authorisation or violating the core principles of Privacy by Design.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Most businesses that handle the personal data of Californians are comes under the data privacy rules "the California Consumer Privacy Act". On January 1, 2020 the CCPA became operative. According to the CCPA, users have right to request that their information be removed, to be informed about and have access to their personal data, and to object to the sale of their personal data. The organization must notify users when their personal data was collected. When a third party sell a user's personal information to another third party, they are also requiring to notify the user. Website can store cookies on user's device without their explicit consent. Permission should be required if the user is under sixteen. Penalties under the CCPA are less severe. impose penalties up to $2,500 for unintentional infractions, $7,500 per intentional infractions, $100-750 in civil court damages.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FRAMEWORK

"The NIST Cybersecurity Framework" was first introduced in 2014 version 1.0. it included a wide range of guidelines related to cybersecurity practices. The new version 1.1 of the NIST Cybersecurity Framework was introduce by NIST in 2018. Version 1.1 of the NIST Cybersecurity Framework included identity verification, authentication and supply chain risk management. National Institute of Standards and Technology cybersecurity Framework the most substantial revision to the framework. The new draft was publicly introduced in 2023 and finalized in February 2024. The new version includes six essential functions: Identity, Protect, Detect, Respond, Recover and Govern. These six principles were introduced to address privacy issues, emphasize continual improvement, and expand the framework's reach to encompass businesses of all sizes and sectors. These six functions are further divided into six categories, it covers areas related to cyber, physical and personal security, with an emphasis on business results.[2] The 108 subcategories are goal-oriented statements that provide direction for creating or improving a cybersecurity program.[3] It will reflect current cybersecurity landscape and provide protection to help manage these risks. These six

[2] National Institute of Standards and Technology (NIST), "Cybersecurity Framework"," *available at*: https://www.nist.gov/cyberframework (last visited on: 10.04.2025)

[3] National Institute of Standards and Technology (NIST), "Cybersecurity Framework"," *available at*: https://www.nist.gov/cyberframework (last visited on: 10.04.2025)

principles will be beneficial for industries, such as financial services like banks, by helping them protect their financial data. It will also help the healthcare sector to protect patient's personal data. It will also help to protect intellectual property and secure the industrial system. The NIST Cybersecurity Framework will also safeguard Government Organizations by protecting vital infrastructure and national security. NIST CSF 2.0 introduced six core functions, a good cybersecurity program depends on each function. A new function called "Govern" was added in NIST 1.1. these pillars help understanding, manage and lower cybersecurity risks. The framework offers a holistic approach to cybersecurity risk management. Each element includes key activities that are vital for building an effective cybersecurity strategy.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

"The DPDP Act" was validated on August 11, 2023. Its main purpose is to safeguard individual's privacy. The European Union's data privacy law, particularly the GDPR, had an impact on the DPDP Act, 2023. However, the DPDP Act was written in accordance with India's data protection regime. "The DPDP Act" will apply worldwide wherever Indian customer's data is collected. It will only apply to personal data that is stored digitally. The Indian Government can impose restrictions on the transfer of data outside India through a notification. "The DPDP Act" also states that anyone can request that their personal data be erased when it is no longer needed. Data fiduciaries must follow this rule unless they are compelled to retain the data for legal or regulatory purposes. However, the government is not obligated to erase personal data in such cases if personal information is necessary for national security, governance, legal requirements, or other statutory needs. Under "the DPDP Act", users have the right to ask data fiduciaries how their data is being processed. User also has the right to request the correction or erasure of their personal data. Additionally, users can nominate a person who will manage data after his death. If a company is processing an individual's data, it should only be for legal purposes and require the customer's consent. To process a minor's data, consent must be obtained from their legal guardian or parents. Lastly, if an individual wants to withdraw their consent for any reason, they have the right to do so. In the case of a data breach, the affected person, along with the Data Protection Board of India and the affected data principal, should be informed. DPDP Act imposes a penalty for non-compliance of up to INR 250 crores; compared to the earlier legislation, the new law has increased the penalty.

Types of Corporate Liability for Data Breaches in India

Under the Information Technology Act, 2000, organisations face both civil and criminal liability if they do not comply with their legal provisions.

Civil Liability

Civil Liability mainly deals with damages and compensation for non-compliance with the IT Act. The IT Act, 2000 addresses "Penalty and compensation for damage to computer, computer system, etc." under section 43 - (1) if someone gains illegal access to a computer, (2) Downloads, copies or extracts any information from a computer or computer system store in any removal storage medium, (3) introduces a computer or network with a virus, (4) the database stored in the computer system has been damaged, (5) interrupts a computer system, (6) refuse or causes the denial of access to any individual allowed to access any computer system by whatever means, (7) facilitates illegal access to a computer, (8) alters the system to charge services to another person's account, (9) destroy, deletes or modifies any data stored in a computer resource adversely impacts it in any way, (10) aims to create harm by stealing, conceals, destroying or altering any computer source. He shall be liable for compensating the aggrieved party for damages pay damages by way of compensation to the person so affected.[4]

According to "Section 43A" of the IT Act, 2000, "Compensation for failure to protect data" - if a business handles, possesses or engages with sensitive personal data in its computer system and, due to its negligence, fails to implement and maintain proper security practices, resulting in wrongful loss or wrongful gain, the company must compensate the affected person.[5]

As per "Section 72A" of the IT Act, 2000, "Punishment for disclosure of information in breach of lawful contract" - if a person or an intermediary obtains personal information while performing services under the lawful contract, they cannot share it without consent. If they do so with the intent to cause or knowing it may cause harm or unfair benefit, they shall be punished with imprisonment, a fine up to five lakh rupees, or both.[6]

Criminal Liability

[4] The Information Technology Act, 2000, Sec. 43
[5] The Information Technology Act, 2000, Sec. 43A
[6] The Information Technology Act, 2000, Sec. 72A

Criminal liability includes fines, imprisonment or both under the IT Act, 2000. Section 66 of the IT Act, 2000 deals with computer-related offences - if any person dishonestly or fraudulently conducts any of the computer-related offences listed in section 43, he shall be punished with imprisonment for a term which may extend to three years or with a fine of up to five lakh rupees or both.[7]

As per section 66 C of the IT Act, 2000, Punishment for identity theft - if someone fraudulently or dishonestly uses another person's electronic signature, password or any other unique identification, they shall be punished with imprisonment of either description for a term which may extend to three years and a fine of up to rupees one lakh.[8]

As per section 66 D of the IT Act, 2000, the Punishment for cheating by personation by using computer resource- whoever cheats by using any communication device or computer resource shall be punished with imprisonment, which may extend to three years and a fine up to be one lakh rupees.[9]

As per section 67 of the IT Act, 2000, Punishment for publishing or transmitting obscene material in electronic form - Whoever publishes or shares in the electronic form can be punished by imprisonment of any kind for a maximum of three years and a fine of up to five lakh rupees upon first conviction, and by imprisonment of any kind for a maximum of ten lakh rupees upon second or subsequent conviction.[10]

As per section 69 A of the IT Act, 2000, the Power to issue directions for blocking public access to any information through any computer resource - (1) any online material can be blocked by the Central Government or an authorised representative if needed for India's integrity and sovereignty, defence and security of the state, friendly relations with other countries, public order, preventing offences associated with these issues. (2) the blocking procedure must adhere specific rules and safeguards as prescribed by law. (3) any intermediary that disregards the blocking order may be fined and imprisoned for up to seven years.[11]

REAL WORLD CASE STUDY

[7] The Information Technology Act, 2000, sec. 66
[8] The Information Technology Act, 2000, sec. 66C
[9] The Information Technology Act, 2000, sec. 66D
[10] The Information Technology Act, 2000, sec. 67
[11] The Information Technology Act, 2000, sec. 69A

Aadhaar Data Leak, 2023

According to a survey conducted by the US cybersecurity firm Security, the dark web has exposed the personal information of 815 million Indians. The threat actor, identified as "pwn0001", stole phone numbers, addresses, aadhaar, and passport information for $80,000. The Central Bureau of Investigation investigated the intrusion. There were indications that the personal information could have come from the Indian Council of Medical Research (ICMR) database. The Government's digitalisation initiatives have been severely hampered by this hack, which has caused a significant setback.[12]

BharatPay Data Breach, 2022

In August 2022, a major data breach exposed the personal data and transaction details of 37,000 individuals from the digital financial services company BharatPay. The leaked data included employees' official email addresses, UPI IDs, Phone numbers, passwords and user names from Indian banking and insurance companies. The breach was identified on August 13 by XVigil, CloudSEK's threat intelligence team. It was discovered on a cybercrime site that BharatPay's database, which contained transaction data, bank balance, and customer personal information, was leaked from 2018 to August 2022.[13]

LEGAL CONSEQUENCES AND PENALTIES FOR CORPORATE DATA BREACHES

Data Breaches occur, causing businesses and organisations to face legal consequences, reputational harm, a loss of consumer trust, and financial losses. The penalty will be imposed for several factors, including non-compliance with the DPDP Act, sharing user data with third parties without consent, and failing to maintain verifiable records of all user consents if the data fiduciary has financially benefited from the breach. The penalty will depend on the nature, gravity and duration of the violation. When failure to inform of a Data Breach, a fine is imposed up to INR 200crores; if failure to meet additional requirements regarding children, a fine of up to INR 200 crores; when a personal data breach occurs imposed fine of up to INR 250 crores; violation of additional obligations significant data fiduciary fine up to INR 150

[12] DPDP Consultants, "Top 5 Recent Data Breaches in India (2024)", *available at*: https://www.dpdpconsultants.com/blog/top-5-recent-data-breaches-in-india-2024-2.php (last visited on: 10.04.2025)

[13] Sattrix, "25 Major Cyber Attacks in India that shocked the nation", *available at*: https://www.sattrix.com/blog/biggest-cyber-attacks-in-india/ (last visited on: 12.04.2025)

crores. The IT Act also imposes penalties for corporate liability on businesses that fail to defend sensitive data. As per section 43A, 72, 72A, 66, 66C, 66D, 67, 69A of the IT Act, 2000.

RECOMMENDATION

1. Adopt best practices from the cybersecurity laws of other countries to help reduce data breaches and cyberattacks.
2. The IT Act does not clearly define several contemporary cybercrimes, such as online stalking, cyberbullying, identity theft and ransomware attacks. There is a need to amend the Act and introduce new cybersecurity policies to prevent data breaches.
3. Establish strict regulations regarding cross-border data transfers.
4. All companies should provide training to their employees on how to prevent personal data leaks to avoid such incidents.
5. All companies should adopt strong security on their computer software to protect against data leaks and hacks.

CONCLUSION

In the growing digital world, individuals are increasingly shifting to the internet. Data breaches have become common incidents nowadays. Companies and organisations face challenges in mitigating cyber threats. India's legal framework, including the IT Act and the DPDP Act, deals with protecting users' personal data. If any company or organisation fails to comply with its liability, i.e., protecting users' personal data, it may face monetary penalties based on the nature and gravity of the breaches. Adopting data protection practices will not only help minimise legal risks but also foster customer trust, prevent financial losses, and enhance long-term business credibility.