

Safeguarding Digital Trust: Corporate Negligence And White-Collar Accountability in India's Data Protection Framework

Dr. Shreemanshu Kumar Dash¹, Ms. Isha Tiwari²

¹Assistant Professor, Law, National University of Study and Research in Law

²5th Year Student of Law (BA.LL.B), Law, National University of Study and Research in Law, Ranchi

ABSTRACT

India has witnessed a fast rate of digitization of its economy, which has made personal data an extremely important corporate asset whose security has become the determinant of consumer confidence and legal compliance. Non-but, in recent years, several cases of data breaches, including the Aadhaar leak, data breach at Zomato, and data exposure of Air India, demonstrate a disastrous trend of corporate negligence, abuse, and structural malfunctions, which is a modern-day variant of white-collar crime. This paper will look at the liability of companies in data breaches according to the Digital Personal Data Protection Act, 2023 (DPDP Act), responsibilities of data fiduciaries in statute, duties in breach notification, and consumer protection processes. It examines the ways in which breaches of sensitive data, underreporting of breaches, and unauthorized use of personal information are both ethical and legal offenses, with a lack of accountability and enforcement. The paper also analyzes the rights of data principals, access, correction, erasure and redressal of grievances and compares the framework of the country with international regulations, like GDPR and CCPA, that offer more mechanisms of enforcement and redress. Major issues that are discussed in order to prove systemic weaknesses in the existing regime are poor institutional supervision, jurisdiction overlap with the IT Act and RBI rules, no criminal penalties, and corporate foaming at the mouth. The paper ends with the proposals of some reforms to make corporations more responsible, such as criminal liability due to gross negligence, Data Protection Board power increase, periodical audits of compliance, technological security and raising public awareness. Being able to frame the issue of data breaches within the framework of white-collar crime, the paper highlights the importance of the balanced approach that would implement strict corporate responsibility and encourage innovation in the Indian digital economy. Finally, it highlights the importance of combining legal, technical, and social actions to ensure the governance of data to provide privacy and ethical corporate conduct.

Keywords: Data, Breaches, Corporate, Negligence, Liability

INTRODUCTION

In the modern digital economy, data is the most important business asset, which drives business decisions, marketing strategies, and innovation. Yet, it is this increasing reliance on personal and consumer data that has also resulted in frightening increase in the number of data breaches in the corporate environment of India. Big e-commerce sites to banks and medical records have seen an

unprecedented spillage of personal details of sensitive nature exposing the millions of users to financial frauds, identity thefts, and privacy invasion. These events disclose a disturbing fact that corporate negligence and profit-oriented data abuse has become a new type of white-collar crime where crimes are perpetrated by not the usual criminals but rather by business organizations and their leaders.

White-collar crimes are generally construed to be financially inclined, non-violent crimes perpetrated by persons of high social status in the process of their occupation. In the digital age, the definition has been broadened to refer to corporate wrongdoing in the form of unauthorized gathering, storage or unsanctioned usage of person-specific data. Although, with the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) a legal framework of data privacy has been introduced, serious compliance and accountability failures are still observed in India. A large number of corporations either do not report breaches in a timely manner or have weak protection mechanisms, and this is an even greater system-wide failure to protect the rights of consumers.

The three key research questions that are going to be answered within the framework of this study are: (1) Is it possible to categorize corporate data breaches as white-collar offenses? (2) What are the provisions of the DPDP Act that deal with the problem of corporate negligence and notification of breaches? and (3) Does the modern framework offer the necessary protection and remedies to consumers? The research questions are to examine the liability of the corporations in the DPDP Act, determine the efficacy of its consumer protection, and examine potential reforms on the enforcement of DPDP.

Finally, this paper holds that corporate negligence when it results in data breach is a new facet of white-collar crime. Although the DPDP Act is a very positive development in law, there are still serious lacunae in application, interpretation, and redress to consumers- and the greater accountability and regulatory attention is needed in the dynamic Indian data control environment.

CONCEPTUAL FRAMEWORK: DATA BREACH AS A WHITE-COLLAR CRIME

White-collar crime was coined by a sociologist known as Edwin H. Sutherland, who defined it as crime committed by a person of status and respectability in the line of duty. This was a huge contrast to the conventional concept of crime where it was mainly linked to physical violence or blatant misbehaviors. In white-collar crimes, on the other hand, there is a deception, misuse of trust, and financial or reputational damage, which is usually committed in the name of legitimate business operations.¹ These offences in the present-day digital economy have not only been limited to financial fraud and insider trading, but also to corporate data abuse, invasion of privacy, and careless data management, which, in combination, can put the security of personal information of individuals in jeopardy.

In this context, corporate crime is not the same as personal crime in terms of magnitude and effects. A company as a legal entity operates through its employees, executives and systems. When the company cannot protect information or intentionally uses it to gain a commercial benefit, it would be involved in an activity that is similar to white-collar criminality, namely, its structural neglect and violation of fiduciary responsibilities instead of willingness to cause harm.² These instances indicate more profound organizational culture of indifference to ethical data practices where the adherence to the data protection norms is not a priority but profit. Therefore, third-party responsibility of data-related white-collar crimes

¹ Edwin H. Sutherland, *White Collar Criminality*, 5 Am. Soc. Rev. 1 (1940).

² S. P. Green, *Lying, Cheating, and Stealing: A Moral Theory of White Collar Crime* (Oxford Univ. Press 2006).

may be considered as the corporate entity itself, and the responsibility may be further extended to the people in the decision-making process and control.

Any such unauthorized access, disclosure, or loss of personal data is called data breach. Such violations can be of various kinds:

1. Unintentional violations, including unintentional sharing or information storage insecurity.
2. Both hackings and insider leaks are intentional breaches as well as deliberate misuse of consumer data.
3. Institutional corporate failures, which occur when the poor security of cybersecurity or poor risk management causes sensitive information to be revealed repeatedly.

The number and severity of data breaches in the Indian context show that this is a problem of serious concern. Such events as the Aadhaar database leak³, Zomato breach (2017),⁴ and Air India passenger data exposure (2021)⁵ have shown the weakness of governmental and commercial organizations. Not only do these breaches invade the privacy rights of the individuals, but also damage the trust that the citizens have on the corporate governance and computer systems.

The negligence of the crime associated with such violations is in the fact that reasonable care was not used and there was no consideration of what is required by law⁶. In the Digital Personal Data Protection Act, 2023⁷, the data fiduciaries have a duty to protect the personal information and disclose any breach. Such a failure will amount to a violation of fiduciary duty and statutory duty, which is consistent with the wider concept of white-collar crime. Hence, during the era of digitalization, data breach is the intersection of technology, ethics, and even criminal law, re-drawing the boundaries of corporate liability and responsibility.

CORPORATE OBLIGATIONS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (the DPDP Act)⁸ represents a significant step in Indian data protection system creation. It imposes significant obligations on corporations which are called Data Fiduciaries, to provide responsible data management and to store the personal information about the individuals. In the Act, a harmonious digital environment is observed in which the rights of individuals (data principals) are protected and creative thought and business growth are supported. However, it is the weighty duty of the compliance on those businesses that gather, store, or handle personal information.

The sections 4 to 8 of the Act⁹ describe the main responsibilities of the Data Fiduciaries. These consist of having free, informed, specific and unambiguous consent of individuals before their personal data is processed, the data is restricted to legitimate and well-defined purposes and restricted to the said purposes- the principle of purpose limitation and data minimization. There is also a need to have a reasonable security check in place by the corporates to prevent unauthorized access, data and abuse.

³ UIDAI Aadhaar Data Leak Controversy: Privacy Concerns Persist, BBC News (Jan. 5, 2018)

⁴ K. Jha, Zomato Confirms Data Breach Affecting 17 Million Users, The Economic Times (May 19, 2017),

⁵ Air India Data Breach: Personal Data of 4.5 Million Passengers Compromised, The Hindu (May 22, 2021)

⁶ Indian Penal Code, 1860, S. 405–409 (India).

⁷ Digital Personal Data Protection Act, 2023

⁸ Id

⁹ Digital Personal Data Protection Act, 2023, S. 4–8 (India).

¹⁰These stipulations may result in massive financial penalties in case of non-compliance, and that is why the legislature may have an interest in turning corporations to suffer in terms of data negligence liability. The introduction of Data Protection Impact Assessment (DPIA) ¹¹of significant data fiduciaries is also introduced by the Act. This is applied to evaluate the risks which are likely to be involved in data processing and to ensure the establishment of preventative measures. Such fiduciaries should also appoint Data Protection Officer (DPO) ¹²who should act as the primary contact regarding redressing grievances and also in ensuring that the organization is adhered to. DPO forms an aspect of corporate accountability, which serves as a channel between the regulators, the management, and the consumers. The other significant aspect of corporate responsibility is breach notification requirement. ¹³The Data Fiduciary must inform the board of India of Data Protection and the affected individuals as soon as there is a breach of data. ¹⁴It is one of the factors that ensure the transparency of the information, enable the implementation of the corrective measures in due time, and enable individuals to mitigate the potential harm associated with the data leaks.

Even as good as these powerful provisions are, there are implementation issues. Many Indian corporations particularly the small and medium enterprises lack mature compliance culture and technical infrastructures that can be used to fulfill the data protection standards. There is also a lot of ambiguity regarding the use of the consent management mechanisms and cross-border data transfer. In addition, ignorance of the aspects of data protection among the corporate orders is also a common cause of accidental violations.¹⁵

Thus, despite the DPDP Act, 2023¹⁶, offering a sound legislative framework on the corporate responsibility of data management, enforcement, corporate willingness, and organizational culture shift with paying attention to privacy and digital responsibility as the elements of business ethics is the only place that it can succeed.

CORPORATE NEGLIGENCE AND LIABILITY IN DATA BREACHES

The issue of corporate negligence during the treatment of personal data has become a burning problem in the digital era. Since corporations are gathering, processing, and storing enormous amount of user data every day, the inability to ensure its safety directly threatens the privacy of the consumer and the trust of the population. The Digital Personal Data Protection Act, 2023 ¹⁷(DPDP Act) acknowledges this weakness and places firm responsibilities on corporations, referred to as data fiduciaries, to be responsible. Nevertheless, within this legal framework, various types of corporate negligence remain relevant in causing repeated occurrences of data breaches in the Indian corporates and governments.

The initial and the most prevalent type of negligence is an inability to protect sensitive data. Lots of companies are using old security measures, poor encryption techniques, and poor training of employees which expose their servers to hacking and unauthorized access. The second type is non-reporting of data breaches which involve organizations that want to avoid reputational losses and fines by knowingly

¹⁰ Id. S. 8(5)(b)

¹¹ Id. S. 10 (requiring assessment before processing high-risk personal data).

¹² Id. S. 9.

¹³ Id. S. 8(6); S. 33

¹⁴ Id. S. 20–21 (requiring reporting of data breaches to the Board and affected individuals).

¹⁵ Nasscom & DSCI, *India Data Protection Readiness Report* (2023)

¹⁶ Digital Personal Data Protection Act, 2023

¹⁷ Id

hiding or delaying the notification of data breaches. This concealment not only goes against the statutory requirements but it also contributes to the damage to the data principals. A third and more heinous variant is the misuse or unauthorized transfer of consumer data to make a profit in which the corporations utilize user information to tailor advertisements, data mining, or sell such information to third parties without consent. These are serious breaches of trust and legality though may be justified as ways of doing business.

Legally, such misconduct is subject to a liability regime with DPDP Act, 2023 creating a clarity regarding that. Section 33 provides a penalty between 250 crore and 100 crore per breach on the corporations depending on the nature and the extent of breach. These fines aim to provide punishment as well as discourage lax data control. The provisions in the Act supplement the provisions that are available under the Information Technology Act, 2000, especially under Section 43A¹⁸ and 72A.¹⁹ Section 43A²⁰ includes the provision that firms dealing with sensitive personal information should act in a manner that is reasonable in respect of security and in case it does not, it will be liable to compensation damages to individuals affected. Section 72A²¹ also criminalizes information disclosure without a consent making the direct connection between corporate negligence and criminal responsibility.

In addition to these laws, there are other laws that corporations can be prosecuted under the Indian Penal Code (IPC). As an illustration, criminal breach of trust is covered under Sections 405- 409²² and cheating and dishonestly inducing delivery of property in Section 420²³. These penal provisions may be applied when corporations abuse personal data or waste the trust of their clients and so the misconduct that seems to be an administrative failure turns into a criminal act.

This has been supported by judicial interpretation of data protection as both a constitutional and ethical responsibility. In *K.S. Puttaswamy v. UOI*²⁴ The recognition of right to privacy as a fundamental right in the Constitution guaranteed by Article 21 of the Constitution²⁵ by the Supreme Court of India (2017), imposes a constitutional obligation on the corporations and the State to protect personal data. Likewise, the Zomato Data Leak (2017)²⁶ and the Aadhaar Data Breach (2018)²⁷ highlighted serious deficiencies in corporate responsibility and compliance to the level that caused people to debate the quality of the data protection ecosystem in India.

Moreover, directors are subject to the duty of due diligence, and they must also make sure that their companies do not break the applicable laws, such as data protection standards, under the Companies Act, 2013²⁸. Data security negligence or failure to guarantee adherence can cause both civil and criminal liability to directors and other key managerial staff.

Overall, data protection negligence by companies is not only a technological error but also a breach of fiduciary, legislative, and ethical responsibilities. The DPDP Act has enhanced the law but effective

¹⁸ Information Technology Act, 2000, S 43A

¹⁹ Information Technology Act, 2000, S. 72A

²⁰ Id

²¹ Id

²² Indian Penal Code, 1860, S. 405, 409, 420 (India)

²³ I.P.C, 1860, S. 420

²⁴ *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

²⁵ Indian const. Art. 21

²⁶ Zomato Confirms 17 Million User Accounts Hacked,' *BBC News* (May 18, 2017),

²⁷ Aadhaar Data Leak: How 1.1 Billion Indians' Data Was Exposed,' *The Indian Express* (May 3, 2018)

²⁸ Company Act, 2013 S.166

responsibility will be based on active corporate management, regulatory supervision and paradigm shift towards regarding data protection as fundamental aspect of responsible business practice.

CONSUMER PROTECTION AND REMEDIES

Essentially, the Digital Personal Data Protection Act, 2023 (DPDP Act)²⁹ is a significant step towards recognizing the rights of individuals, who are called, data principals, in the Indian system of data governance. The Act will empower the consumers since they will have a significant level of control over their personal information besides ensuring accountability among the corporations. However, despite the law presenting several consumer oriented requirements, there remains a great level of doubt that such provisions would be effective in practice because they are not accompanied by enforcement measures, are fraught with time wasting processes, and lack of awareness among consumers.

There are several basic rights of data principal³⁰, which are designed to ensure their privacy and autonomy with the DPDP Act. They are the right to information, in which the individuals are entitled to know how their data is collected, accessed and stored, the right to correction and erasure, in which the user has a right to correct any mistake and demand the data fiduciaries to delete unnecessary redundant data or data which is no longer required; and the right to grievance redressal, whereby the fiduciaries of the data are under obligation to present readily available channels through which the consumer can complain. On their own, they are the pillar of digital empowerment of individuals in order to have them be active actors in how they manage their personal information as opposed to passive subjects.

The Act offers a formal breach reporting and recovering process in case of data breaches. Data fiduciaries in the form of corporates must make sure that they report to Data Protection Board of India (DPBI) and affected persons in case of data breach promptly. The DPBI is a significant adjudicatory and enforcement organization that investigates the breaches of the Act, fines and imposes the Act.³¹ However, the absence of an outright structure of rewarding the victims is among the issues that had lingered. As compared to the earlier Information Technology Act, 2000³², on the question of compensation, the DPDP Act implies the imposition of the administrative penalties as a substitute of individual redress. This puts a massive gap between effective and timely redressing to the consumer victims.³³

India appears not as thorough as its counterparts all over the globe. The right to claim damages of either material or non-material, in case the data of people is abused, is the right of the European Union.³⁴ Likewise, the California Consumer Privacy Act (CCPA)³⁵ allows the consumer to receive civil damages in case of a data breach and forces corporations to disclose information on a high standard. The two models emphasise on transparency, enforceability and consumer empowerment which is quite weak within the Indian legislative system.³⁶

The case studies of the recent corporate breaches of the corporations in India, i.e. Zomato (2017)³⁷ in data leaks and Air India (2021)³⁸ data leak have demonstrated that the responses of the corporations were

²⁹ Digital Personal Data Protection Act, 2023

³⁰ Digital Personal Data Protection Act, 2023, S. 11–14

³¹ Id S.19

³² IT Act, 2000

³³ NITI Aayog, *Data Empowerment and Protection Architecture (DEPA) Report* (2020).

³⁴ Regulation (EU) 2016/679, General Data Protection Regulation, arts. 33–34, 82, 2016 O.J. (L 119) 1

³⁵ California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2020)

³⁶ CyberPeace Foundation, *Corporate Response to Data Breaches in India* (2023),

³⁷ Id Zomato Data Leak,

quite sluggish and inadequate. The majority of the affected consumers never even knew their rights or remedies to seek redressal. This indicates an even greater issue of consumer ignorance and the need to work proactively by recruiting the government and corporations into the task of enlightening the people on their digital rights.

In this regard, the DPDP Act will have an informational background in safeguarding consumers, although its effectiveness will depend on strengthening the enforcement processes, introducing the concept of compensatory reparations, and forming a more aware consumer. Only then, the Act will be capable of achieving its goal of bringing justice and accountability to the domain of digital privacy.

ENFORCEMENT CHALLENGES AND POLICY GAPS

Despite the quite comprehensive framework of the Digital Personal Data Protection Act, 2023³⁹ (DPDP Act), there are several structural and systemic issues to the provision of their provisions. Despite the fact that the Act is making some attempts to make companies more responsible and enhance the privacy of consumers, the unavailability of effective enforcement procedures, overlaps of jurisdictions, and institutional independence continue to affect the negativity against its effectiveness. The loopholes given above will jeopardize the DPDP Act as a symbolic reform as opposed to a revolution in Indian data protection laws.

One of the challenges also includes weak enforcement mechanism of the Act⁴⁰. There is lack of clear independence and structural autonomy of Data Protection Board of India (DPBI) that is envisaged to be the main adjudicative body in case of violation of data protection. The composition, appointment procedure as well as its functions are highly controlled by the Central Government. The issue of such dependence is of special interest to impartiality and regulatory capture especially when it involves large corporate entities. Moreover, the Board power is mostly administrative and does not have much power to investigate and prosecute. This kind of loose discretion of power in cause and effect is subverting deterrence, and weakening corporate responsibility.

The other issue is anchored on overlaps of jurisdictions of the DPDP Act⁴¹ with the existing regulations such as the information technology act, 2000 and the data protection regulation of the central bank of India (RBI) data protection regulations. Citing the example, the lack of the protection of data is already covered by the IT Act, section 43A,⁴² and RBI demands financial institutions to localize their data and establish the requirements of cybersecurity. These regimes have no definite division of powers that confuse in implementing the authority and corporations utilize gaps at the expense of taking advantage of the loopholes in the regulations.

It is also worrying that there are no criminal penalties in the event of severe breaches. The DPDP Act is primarily concerned with the cases of administrative failure in the instances of data breach that are associated with the means of financial penalty, rather than criminal prosecution. Nevertheless, in most jurisdictions with respect to the GDPR, purposeful or gross negligence misuse of data is a criminal act, in comparison to other jurisdictions such as those within the European Union. India does not have such kind of deterrence and the companies view the fines as a cost of business and not a risk of being careless.

³⁸ Id Air India

³⁹ Digital Personal Data Protection Act, 2023

⁴⁰ Digital Personal Data Protection Act, 2023, S. 27.

⁴¹ Reserve Bank of India, *Master Direction on IT Framework for NBFCs* (2023).

⁴² IT Act 2000, S. 43A

There is also the problem of corporate influence and necessity to avoid following the regulations. The majority of the companies neither report nor delay the notification of breaches but rather minimise the scale of the incidence to protect their image on the market. The behaviour is also encouraged by the fact that DPBI also has few capabilities regarding investigations, thereby contributing to the slowness of consumer warnings and redressal problems.

To seal these gaps, there is an urgent necessity to have more institutional integration and coordination between the institutions such as the Indian Computer Emergency Response Team (CERT-In), ⁴³the law enforcers and the DPBI. A single system of data governance would enable a quick response to incidents and offer consistency in enforcement and sharing of technical expertise.

In conclusion, despite the fact that the DPDP Act is a good lawmaking project, its results will be restricted to the strengthening of the authority to enforce and regulate the willful corporate crimes making regulation independent and offering criminal prevention to such offenses. Without these reforms, the Indian data protection regime will still remain reactive and not preventative, which not only destroys consumer confidence but also integrity of digital ecosystem.

THE WAY FORWARD: REFORMING CORPORATE ACCOUNTABILITY

To effectively manage the corporate negligence India should not stop on administrative punishment, but execute a multi-dimensional response to corporate negligence by fencing and controlling the corporate negligence in data breaches. Bringing about criminal liability in gross corporate negligence during major breaches is among some of the key reforms⁴⁴. Whereas DPDP Act has monetary fines, criminal punishment would be an effective deterrent measure to intentional or negligent failure to observe data protection obligations. This would place India at the same level with the rest of the world and make people remember the extent of privacy invasion as white-collar crime.

The other desirable action is the reinforcement of the Data Protection Board of India (DPBI). The powers bestowed by giving the Board more investigative abilities and institutional autonomy would enable the early detection, assessment, and sanctioning of breaches. Speaking of which, conducting regular compliance audits on large data fiduciaries would ensure that security practices, breach preparedness, and compliance with statutory requirement take effect and ensure that the issue of systemic failures is reduced.

Specialized compensation fund can be established in order to make sure that individuals who have become the victims of data breach can be compensated at the right moment to provide additional consumer protection. This would also complement the adjudicatory role of the DPBI and direct assistance to the victims to fill in one of the major gaps in the current system in India.

Another important thing is to enhance data ethics and transparency in the corporation. The companies, in their turn, are required to possess sound internal data handling responsible policies and publicly disclose their data handling policies and breach cases. The technological defense (such as the implementation of strong encryption), artificial intelligences (AI) to identify breaches, and the choice of localization of data would reduce the susceptibility to cyber attack and increase the reliance on online resources.

Finally, publicity and education of the consumers should be present. Citizens should be sensitized on their rights in the DPDP Act and made to act and hold companies to book. The awareness programs, the

⁴³Indian Computer Emergency Response Team (CERT-In), *Guidelines on Information Security Practices* (2022).

⁴⁴Shreya Sinha, 'Corporate Negligence and Data Privacy in India,' *The Wire* (Sept. 14, 2023)

current grievance mechanisms, and the digital literacy programs can be integrated and enable the users to have a say in the establishment of a responsible data environment.

In conclusion, corporate responsibility needs reforming, and this should be assisted by a package of legal, technological, and social actions. India can establish a strong digital ecosystem in which data protection has become a core element of corporate governance and white-collar crime prevention through making gross negligence a criminal offense, making institutions control the conduct of corporate ethics, and empowering the consumers.

CONCLUSION/ SUGGESTION

In India, information theft has become one of the most critical forms of white-collar crime, which is a demonstration of corporate carelessness, intentional abuse or systematic failures that undermine personal information on a colossal level. The comparison of the Aadhaar breach, Zomato data leak, and Air India data exposure shows that such breaches are not technical failures but can be used to show more profound fiduciary, statutory, and governance failures within corporate environments. The changes emphasize the importance of having a strong legal and regulatory framework such that the organizations are responsible and at the same time, protect the rights and interests of consumers.

The Digital Personal Data Protection Act, 2023 (DPDP Act) sets the stage of India in the journey of being digitally accountable. The introduction of corporate responsibility and consumer protection mechanisms by the Act requires data fiduciaries to clearly state their duties and responsibilities, obligate prompt breach notifications and create the Data Protection Board of India. Nonetheless, there are still critical gaps despite such precautions. The laxity of the law is decreased by weak enforcement, lack of effective criminal sanctions, and slow or poor redress, and lack of a corporate compliance culture. These restrictions will not help without enhanced institutional regulation that would prevent corporations to consider penalties as a business expense, not an incentive to avoid laxity or wilful violations.

In order to overcome these deficiencies, a number of reforms are needed. The concept of criminal responsibility ought to be brought in to cases of gross corporate negligence in significant data breaches, so that indifferent or intentional infraction can be regarded as a punishable crime rather than a monetary one. The Data Protection Board must be given more power to conduct proactive investigations, enforcement, and supervision. Corporations must be obliged to perform routine compliance audits, introduce sophisticated technological protection measures, including encryption, AI-assisted breach identification, and data localization, and have open disclosure policies. Moreover, the establishment of a compensation fund among aggrieved consumers would be a relief that would help in enforcing the aspect of accountability.

The second one is the need to promote consumer awareness and digital literacy. By raising awareness in people about their rights to access their data and the redress mechanisms, it is possible to make sure that the protection of privacy does not only constitute a statutory duty but a social expectation as well. Data protection can be made more of a civic involvement than it is a company regulation through awareness campaigns, hinged on an available system of redressing grievances, and education programs.

The final, and arguably the most serious, problem is how to strike the right compromise between a set of strict data protection rules, white-collar crimes, and ethical business conduct on one hand, and the promotion of innovation and the development of the digital economy in India, on the other. India can convert DPDP Act into a very strong regulatory body into an ethical, accountable and secure digital governance by providing a bridge between the statutory requirements and the practice. This would not

only help in alleviating the effects of corporate negligence but also help build a more robust trust among the people, as the technological development will be achieved through proper management of personal information.

REFERENCES

1. Acts and Statutes (India)

1. **Digital Personal Data Protection Act, 2023**, No. 22, Acts of Parliament, 2023 (India).
2. **Information Technology Act, 2000**, S. 43A, 72A (India).
3. **Indian Penal Code, 1860**, S. 405, 409, 420 (India).
4. **Companies Act, 2013**, S 166(3) (India).
5. **Reserve Bank of India**, *Master Direction on IT Framework for NBFCs* (2023).
6. **Reserve Bank of India**, *Circular on Storage of Payment System Data* (Apr. 6, 2018).
7. **California Consumer Privacy Act of 2018**, Cal. Civ. Code S 1798.100–1798.199 (West 2020).
8. **Regulation (EU) 2016/679**, General Data Protection Regulation, arts. 33–34, 82, 2016 O.J. (L 119) 1.

2. Case Law

1. **K.S. Puttaswamy v. Union of India**, (2017) 10 S.C.C. 1 (India).

3. Journals and Academic Articles

1. Edwin H. Sutherland, *White-Collar Criminality*, 5 Am. Soc. Rev. 1 (1940).
2. M.P. Gupta, *White Collar Crime in India*, 7 J. Ind. L. Inst. 323 (1965).
3. Shreya Sinha, *Corporate Negligence and Data Privacy in India*, *The Wire* (Sept. 14, 2023), <https://thewire.in/law/corporate-negligence-data-privacy-india>.

4. Reports and Policy Documents

1. NITI Aayog, *Data Empowerment and Protection Architecture (DEPA) Report* (2020), <https://www.niti.gov.in/>.
2. NITI Aayog, *India's Digital Economy Report* (2023), <https://www.niti.gov.in/>.
3. Nasscom, *India Data Protection Readiness Report* (2023), <https://www.dsci.in/>.
4. Nasscom, *Recommendations on DPDP Rules, 2024 Draft* (2024).
5. Ministry of Consumer Affairs, *Digital Consumer Rights Initiative Report* (2022), <https://consumeraffairs.nic.in/>.
6. CyberPeace Foundation, *Corporate Response to Data Breaches in India* (2023), <https://www.cyberpeace.org/>.
7. OECD, *Good Practice Principles on Data Governance* (2021), <https://www.oecd.org/>.

5. News Articles and Online Sources

1. “‘Aadhaar Data Leak: How 1.1 Billion Indians’ Data Was Exposed,’ *The Indian Express* (May 3, 2018), <https://indianexpress.com/article/technology/tech-news-technology/aadhaar-data-leak-issues-explained/>.
2. “‘Zomato Confirms 17 Million User Accounts Hacked,’ *BBC News* (May 18, 2017), <https://www.bbc.com/news/technology-39965547>.
3. “‘Air India Data Breach Exposes Data of 4.5 Million Passengers,’ *The Economic Times* (May 21, 2021), <https://economictimes.indiatimes.com/news/india/air-india-data-breach/>.