IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CORPORATE CRIMINAL LIABILITY FOR DATA MISUSE: EXPLORING LEGAL MECHANISMS, REGULATORY GAPS, AND ENFORCEMENT CHALLENGES IN INDIA'S DIGITAL ECONOMY

Student of LLM- Jyoti Sisodiya, LLM, Lingayas' Vidyapeeth Dr. Monika Rastogi
Professor & Head School of Law Lingaya's Vidyapeeth ms. Ruchi kaushik
Assistant Professor
School of Law Lingaya's Vidyapeeth Faridabad, Haryana, India

ABSTRACT

Personal data is an asset or a product of high economic value. Furthermore, there is a correlation between the level of trust and the protection of specific data from personal life. In India, criminals have developed as a major concern for businesses with rapidly expanding business sectors and increasing numbers of corporate fraud cases. This report provides a comprehensive analysis of criminal liability for Indian companies. In the Modern era, corporate crime has become a bigger problem for the judiciary system as a whole. Personal data protection is not currently regulated by other laws, but continues to be distributed among a variety of laws and regulations. Legal provisions relating to the protection of personal data remain sector based. It appears that in the context of privacy, optimal and effective protection could not be provided. If you see a victim of a corporate crime for the criminal act of escaping personal data, it is very natural that the company must be responsible for all of its actions. The guilt of crime comes from the saying. Legal proverb: "Actuated Non-Fast Rium Nishi men's sitting means that their actions will not be considered illegal if they are committed in an illegal state of mind. This is the basis of criminal responsibility. These are business related crimes committed by organizations. India can learn from other countries to improve its legal system and increase the responsibility of businesses to protect its financial system. Bad regulations and gaps in India have led to famous incidents and economic mistakes. The types of losses and impact of corporate crimes are felt later (of

actual victims) and seen later (by potential victims). Competitive businesses, customers, and the general public are among the victims of corporate crime. This research paper examines data abuse and gaps and challenges, controversy, law, and criminal liability for data for Indian judgments.

INTRODUCTION

In 1890, the Harvard Law Review published an essay by Samuel Warren and Louis Brandeis tilted "The Right to Privacy," which established the idea of the right to private. As part of the human rights debate, they advocated for the recognition of the "right to be left alone" as an individual right and contended that it had to be safeguarded by current legislation. The legal adage "Actus Non Facit Reum Nisi Mens Sit Rea" applies to corporate crimes, indicating that the accuser's purpose and actions are necessary to show guilt. This rule alone is insufficient since it has various restrictions. First, it must be proven in a court of law that what is banned by law. As a result, although the right to privacy has been acknowledged, its definition remains elusive. As a component of human rights, privacy recognizes the safety of personal information as a crucial right. In addition to being significant, the right to privacy via data protection is also a crucial component of personal liberty and dignity. The attainment of political, spiritual, religious, and even sexual freedom is strongly influenced by data privacy. This obligation may extend to a number of legal laws, such as those outlined in the Information Technology Act of 2000 and the Indian Penal Code (IPC). In essence, even if the persons directly responsible for data exploitation are not convicted, organizations can still be held liable

Meaning of corporate criminal liability data misuse:

Corporate criminal responsibility for data abuse implies that a firm can face criminal charges for the illegal use, disclosure, or theft of data by its employees or agents operating on its behalf. This responsibility is often confined to conduct performed in the course of employment and designed to benefit the company. Corporate criminal responsibility, arises when a company's workers or agents commit a crime while acting in the course of their job and, to some extent, for the company's advantage.

Examples of data misuse:

This may involve data theft, unauthorized access to personal information, or the use of data for criminal objectives such as fraud or insider trading.

Personal data leaks can occur owing to internal disclosures as well as external attacks. The public was shocked by the widespread circulation of President Jokowi's vaccination certificates on social media, which included his population identification number (NIK), name, date of birth, vaccine date, and type. This was extensively shared on social media, which is horrible. It's important to demonstrate that relying only on one party's assertion is insufficient. Other parties or relevant agencies must also provide evidence. The government acts through sectoral agencies in line with the authority authorized by law oversees the protection of the public's personal data. They are concerned that the public may perceive firms and linked authorities as lack-

ing legal understanding in protecting personal data. Data leaking can be caused by unauthorized access, interception, or man-in-the-middle attacks, as per criminal legislation. However, leaking might also be caused by an insider's conduct. Insiders are responsible for maintaining the confidentiality of user data when sending it outside of the system. The corporation, as the controller and data processor, is responsible for both physical and logical security systems.

So in this research paper it will be discussed corporate criminal liability for data misuse and what are the regulatory gaps, challenges and enforcement mechanisms.

METHOD

The research in this paper is carried out using normative legal research methods. This type of quote jurist study considers many formal legal standards, including laws and regulations related to the concerns presented. This research report was developed using legal, conceptual, and comparative approaches.

.

CONTENT

We, belong to a world that collects and stores data everywhere. Modern computer technology enables us to learn and retain knowledge, interact instantaneously and internationally, purchase products and services, pursue interests, and engage in politicians and social issues, all in lesser time and at a lower cost than previously thought feasible. The revolution has significantly reduced individuals' rights as well as demands of privacy. Vendors, service providers, and government agencies now gather and keep data about transactions involving individuals ("Consumers"), revealing more personal information than was previously possible. Retaining data increases the possibility of third parties obtaining information without the consumer's consent, including criminal hackers, and multinational organizations. The risk exists when individuals in possession of Data may not appropriately protect it or choose to leak it for personal advantage.

The reason should corporate criminal liability matter: -

Corporate criminal responsibility serves a number of significant uses:

- Prevents Wrongdoing: The possibility of legal punishment can prevent businesses and their employees from participating in illegal activities.
- Safeguards the Public Interest: It makes companies responsible for activities that hurt individuals or the natural world.

- Increases Ethical Behavior: It promotes businesses to adopt strong compliance processes and ethical company standards.

Conditions required establishing corporate criminal liability

- Act should be committed by an employee or servant.
- It should be during the course and ambit of employment.
- It should be done in the order to benefit the company/ corporation.

Case judgments

In India, corporate criminal responsibility for data abuse can be proven through a variety of legal means. An important case are:-

- *Naveen Kumar R @ Naveen & ANR and State of Karnataka*, in which workers were prosecuted with data theft in breach of non-disclosure agreements, illustrating the criminal repercussions of such behavior.
- The *Iridium India Telecom Ltd. v. Motorola Inc*, decision established that organizations can be held criminally accountable for their employees' conduct, even if those actions were not approved.
- The Jagjeet *Singh v. State of Punjab and Anr*. Case demonstrated that data theft and hacking, even while covered by IT legislation, can result in penalties under the Indian Penal Code.
- *Standard Chartered Bank vs. Directorate of Enforcement (2005):* The Supreme Court ruled that a business can be tried and penalized for crimes punishable by jail, even if it cannot be imprisoned itself. This was a watershed moment because it challenged the long-held belief that corporations are free from criminal culpability.

Legal mechanisms

Corporate criminal responsibility, for data abuse is created by a variety of legislative measures, including the Indian Penal Code (IPC) and the Information Technology Act of 2000. The Digital Personal Data Protection Act of 2023 (DPDP Act) enhances this liability by holding corporations responsible for data breaches and poor security measures.

Key Legal Provisions:

- The Indian Penal Code (IPC):-The IPC, created in 1860, recognizes businesses as legal organizations and holds them accountable for crimes such as fraud, forgery, and criminal breach of trust.
- Information Technology Act of 2000:- Sections 43 and 43A, organizations accountable for cyber-crimes and data breaches, addressing data protection and cyber security issues. Section 43 penalizes people for unlawful access, downloading, and damage to computer systems and data, but Section 43A, holds corporations accountable for poor security of sensitive personal information.
- The Digital Personal Data Protection Act, 2023 (DPDP Act):- requires data fiduciaries (organizations that handle personal data) to maintain strict security policies and hold them liable for breaches and illegal access. Failure to deploy proper security measures might result in penalties as high as 200cr rupees.
- IT Act:-Section 72A, causes firms liable for any illegal disclosure of personal data.

Corporate criminal liability in India is governed by a legislative framework. Let us break them down:

Companies Act, 2013:-

- Section 447 outlines harsh consequences for companies that engage in fraudulent acts, including fines and imprisonment for responsible executives.
- Section 248 - Noncompliance and Misrepresentation: The Registrar of Companies has the authority to strike off a corporation for chronic noncompliance.

The Prevention of Corruption Act of 1988 (Amended 2018):-

- Establishes corporate accountability for bribery, resulting in criminal prosecution for companies found guilty of bribery against public officials.
- To avoid responsibility, corporate organizations must demonstrate "adequate compliance methods"

SEBI Regulations and White Collar Crimes:

- Insider trading, market manipulation, and deceptive activities expose corporations to legal jeopardy.
- Noncompliance results in SEBI investigations, debarment, and significant penalties.

The Environment Protection Act of 1986:-

- Established strict criminal culpability for environmental damage, regardless of intent. Directors and officials may be personally prosecuted for environmental carelessness.
- These rules clearly demonstrate a move toward greater enforcement and corporate responsibility.

Global Comparison: India's Compliance with International Standards: -

- UK Bribery Act, 2010:-
  - Failure to Avoid Bribery" - Companies may face prosecution when they fail to enforce sufficient anti-bribery practices.
  - Similar to India's Prevention of Corruption Act (2018) revisions.
- The US Foreign Corrupt Practices Act (FCPA):-
  - Allows firms to be punished for offenses done outside the US.
  - Indian enterprises operating abroad must comply.
- France's Sapin II Law
  - Mandates anti-corruption compliance systems for major corporations, while India is also implementing comparable corporate governance changes.
  - While India is coming up to global norms, rigorous liability and corporate compliance requirements are developing.

Corporate Liability and attribution:

- Corporate criminal responsibility is based on, the "directing mind and will" theory. This means that a corporation can be found accountable if an offense is committed by a person or group in charge of its activities.
- "Body Corporate":
  The IT Act defines a "body corporate" as any business, firm, single proprietorship, or other organization of persons involved with commercial or professional activity.

Regulatory Gap

Corporate criminal liability, gaps occur largely because it is difficult to prove "mens rea" (criminal intent) in commercial situations, there is no particular law addressing some crimes such as corporate homicide, and there are no new sentence alternatives beyond fines. Furthermore, legislative fragmentation and the problems of enforcing fines might exacerbate these inequalities.

1. Difficult Proving Mens Rea.

- Corporations are legally entities rather than individuals, and their ways of making decisions include many people, making it difficult to prove their criminal intent (mens rea).
- A corporation's "mens rea" is frequently attributed to the activities of its high-level workers, although it can be difficult to demonstrate that these persons acted with the requisite unlawful intent, as reported by the International Journal of Law.
- The "identification theory" is employed in certain countries to assign the mens rea of high-level executives to the business, although it has limits.

2. The lack of specific legislation:

- In India, the Indian Penal Code (IPC) does not cover all business crimes, and there is no explicit statute regulating corporate murder.
- In accordance to the National Law School of India University, the lack of particular regulation might open up opportunities for businesses to avoid responsibilities and negotiate lower fines.
- Other jurisdictions have similar gaps, with some nations missing explicit legislation for some forms of commercial crimes, in accordance to the National Institutes of Health (NIH) (.gov).

3. Limited Sentencing Options:

- While fines are a popular penalty for corporate crimes, they may not effectively prevent misbehavior or offer substantial reparation to victims.
- Alternative punishment alternatives, such as community service, corporate probation programs, or certain sorts of repair, may be more successful in addressing corporate wrongdoing and increasing responsibility.
- According to IJCRT, the financial burden of executing penalties may divert resources away from different components of law enforcement.

4. Regulatory Fragmentation and Enforcement Issues:

- Multiple regulatory authorities, with overlapping jurisdictions can cause miscommunication and ineffectiveness in enforcement operations, according to IJCRT.
- Communication among regulatory organizations is required to guarantee complete monitoring of company operations and successful execution of legislation.
- Enforcing fines can be difficult, especially when the firm is not profitable, and this can result in enforcement gaps.

Corporate criminal responsibility for data misuse in India, poses major enforcement issues due to the diversity of digital activities, the necessity to access data kept across borders, and the constantly shifting nature of technologies. While legislation such as the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 target data leaks and abuse, implementing them on global firms operating in India may be challenging. In addition, the necessity to combine data privacy with regulatory demands, as well as the possibility of AI-driven criminal activity, complicates matters

.

Challenges in enforcement include geographic and technological barriers.

- Geographic and Technological Barriers:-Global technology businesses frequently keep records in foreign countries, making it harder for Indian authorities to obtain and examine breaches of information.
- The complexity of digital processes: - including the usage of AI can make it challenging to identify the origin of data exploitation and assess a company's liability.
- Balancing Data Privacy and Enforcement: - Law implementation organizations must strike a balance between accessing data and protecting people' privacy, which might provide legal challenges.
- Evolving technology and AI:-The fast growth of technology, especially AI, creates new issues for data security and compliance. Machine learning techniques may be exploited to gather and abuse data.
- Need for International Cooperation:-International collaboration is necessary for investigating and prosecuting data breaches that involve attackers or devices located outside of India.

Protection Strategies:

- Strengthening data protection laws.-Enforcing and strengthening current regulations, including more rigorous measures for breach of data and penalties.
- Improving Cyber security: - Encouraging enterprises to adopt strong cyber security procedures to prevent data leaks.
- Promoting International Cooperation:-International cooperation, involves sharing information and coordinating inquiries into international data breaches.
- Investing in technological literacy: - involves educating the public on the significance of security and privacy of data.
- Creating Ethical AI Frameworks: - Developing norms and regulations to avoid AI from being utilized for illicit purposes.
- Improving Enforcement Mechanisms: - Giving law implementation authorities the tools and funds to investigate and punish data abuse incidents.

CONCLUSION

The Indian Corporate Legal System lacks clarity on Corporate Crimes, under the Indian Penal Code, 1860. The Indian Penal Code, 1860 has not been amended. Also, Indian legal the current system lacks a clear list of Corporate Criminal Liability, allowing for potential escape routes. The Code of Criminal Procedure (CrPC) and Indian Penal Code do not clearly define the responsibilities of Directors and Managerial Personnel in key roles inside the organization. Private Information is a very valuable commercial asset or commodity. Furthermore, there is a connection between trust levels and the safeguarding of personal data. Personal data protection is not presently managed by a distinct legislation, but rather by a variety of regulations and statutes. Legal measures relating to the safeguarding of personal data remain limited and partial; it appears that they have failed to offer optimum and successful safeguarding of private data as a form of privacy.

Considering those harmed of corporate crime, in the unlawful conduct of broad personal data leakage, it is only logical that the business be held accountable for all of its acts. Corporate crimes can have long-term ramifications for both current and future victims. Corporate criminality affects rivals, consumers, and the public at large.

REFERENCES

1. Wahyudi Djafar and Asep Komarudin, Perlindungan Hak Atas Privasi di Internet: Beberapa Penjelasan Kunci. Jakarta: Elsam, 2014.
2. Freeman M and Ert G. International Human Rights Law. Canada: Irwin Law Inc., 2004.
3. Huda C. From Pidana Tanpa Kesalahan to Pidana Pertanggungjawaban, Cet. Kedua. Jakarta: Prenada Kencan, 2006.
4. Saleh R. Tindak Pidana dan Pertanggungjawaban Pidana", Jakarta: Aksara Baru, 1983.
5. Marpaung L. Proces Penanganan Perkara Pidana. Jakarta: Sinar Grafika, 2011.
6. Jayawickrama N. The Judical Application of Human Rights Law (National). United Kingdom: Regional and International Jurisprudence; 2006.
7. Muis Ari Guntoro, Sanusi Sanusi, Fajar Ari Sudewo. Corporate Criminal Liability for Leakage of Personal Data