



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BALANCING PRIVACY AND PUNISHMENT: A COMPARATIVE STUDY OF CRIMINAL LIABILITY IN DATA PROTECTION LAW

~ *Gauri Chauhan*

ABSTRACT

The rapid expansion of digital ecosystems has transformed personal data into one of the most valuable contemporary assets, simultaneously intensifying concerns relating to privacy, security, and accountability. Legal systems across the world have responded by developing diverse enforcement mechanisms designed to regulate the collection, processing, and misuse of personal information. While jurisdictions such as the European Union, the United Kingdom, and the United States continue to employ regulatory models that combine administrative sanctions with targeted criminal liability for serious data-related misconduct, India's enactment of the Digital Personal Data Protection Act, 2023 represents a notable departure through its predominantly decriminalized enforcement structure.

This paper undertakes a comparative legal analysis of India's data protection enforcement framework against selected international jurisdictions in order to examine the implications of decriminalization on regulatory accountability. The study first evaluates the European Union's rights-based regulatory architecture under the General Data Protection Regulation, followed by an examination of the United Kingdom's hybrid enforcement model under the UK Data Protection Act 2018, which integrates administrative penalties with criminal sanctions for specific violations. It further analyses the sectoral regulatory approach adopted by the United States, with particular reference to the Health Insurance Portability and Accountability Act of 1996 and related federal enforcement mechanisms.

Through comparative analysis, the paper identifies the strengths and limitations of India's current framework and explores whether the complete absence of criminal liability may weaken deterrence in cases involving deliberate, malicious, or egregious misuse of personal data. The study ultimately proposes a balanced reform-oriented model aimed at strengthening

accountability while preserving regulatory efficiency within India's evolving digital governance framework.

Keywords: Data Protection, Privacy Law, Criminal Liability, Comparative Legal Analysis, Regulatory Enforcement, Digital Personal Data Protection, Data Governance

CHAPTER 1: INTRODUCTION AND RESEARCH FRAMEWORK

1.1 INTRODUCTION

The digital age has fundamentally altered the manner in which personal information is collected, processed, stored, and exchanged. Governments, corporations, healthcare institutions, financial entities, and digital platforms increasingly depend upon large-scale data processing for operational efficiency, economic growth, and technological innovation. However, this unprecedented reliance on personal data has also generated significant legal and ethical concerns relating to privacy, unauthorized access, identity theft, surveillance, and data exploitation. As personal data becomes an essential economic and strategic resource, ensuring effective legal accountability for its misuse has emerged as a global regulatory priority.

In response to these evolving challenges, jurisdictions across the world have developed diverse data protection frameworks designed not only to safeguard informational privacy but also to establish mechanisms for enforcement and accountability. The European Union has adopted a comprehensive rights-based regulatory structure under the General Data Protection Regulation, emphasizing stringent compliance obligations, administrative penalties, and robust institutional oversight.¹ Similarly, the United Kingdom has retained a hybrid enforcement framework under the UK Data Protection Act 2018, combining civil regulatory mechanisms with targeted criminal sanctions for serious or deliberate violations.² In contrast, the United States follows a sector-specific regulatory approach, where criminal liability is imposed selectively through statutes such as the Health Insurance Portability and Accountability Act of 1996 and other federal laws governing sensitive data sectors.³

Against this global regulatory backdrop, India introduced the Digital Personal Data Protection Act, 2023 as its first comprehensive legislative framework dedicated to personal data

¹ European Parliament and Council, *Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Official Journal of the European Union, L119/1 (2016).

² United Kingdom, *Data Protection Act, 2018* (c.12), HMSO, London

³ United States Congress, *Health Insurance Portability and Accountability Act, 1996*, Pub. L. No. 104–191, 110 Stat. 1936.

protection.⁴ While the Act represents a significant legislative milestone in India's digital governance journey, one of its most distinctive features is its departure from traditional penal enforcement mechanisms. Unlike several mature jurisdictions that retain criminal sanctions for intentional or aggravated data-related misconduct, India's framework primarily relies on administrative penalties and regulatory compliance measures, thereby reflecting a policy preference for decriminalization.

This shift raises important questions regarding the adequacy of India's enforcement architecture, particularly in addressing deliberate, malicious, or repeated violations involving sensitive personal data. In this context, a comparative examination of international enforcement models becomes essential to assess whether India's current approach effectively balances innovation, compliance, and accountability. Accordingly, this study critically analyses India's decriminalized framework in comparison with the European Union, the United Kingdom, and the United States, with the objective of identifying best practices and proposing a balanced reform model for strengthening criminal accountability in Indian data protection law.

1.2 OBJECTIVES OF THE STUDY

The present study seeks to critically examine the position of criminal accountability within India's emerging data protection regime through a comparative legal perspective. Specifically, the study aims:

1. To comparatively examine the criminal and regulatory enforcement mechanisms adopted by the European Union, the United Kingdom, and the United States in addressing serious data-related violations.
2. To identify the strengths, limitations, and policy implications of India's decriminalized approach in comparison with mature international regulatory frameworks.
3. To propose a balanced and context-sensitive reform model capable of strengthening criminal accountability within India's evolving data protection framework.

1.3 RESEARCH METHODOLOGY

This study adopts a doctrinal and comparative legal research methodology to critically examine the evolving framework of criminal accountability in data protection law. The doctrinal component of the research focuses on discovering, analysing, interpreting, and synthesizing

⁴ India, *Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023), Gazette of India, New Delhi.

the law as it presently exists through the examination of statutory provisions, regulatory frameworks, policy documents, judicial interpretations, and scholarly literature. This approach enables the identification of conceptual ambiguities, legislative gaps, structural inconsistencies, and policy limitations within existing legal texts.

In addition to doctrinal analysis, the study employs a comparative legal approach by systematically examining India's regulatory framework alongside established international jurisdictions, namely the European Union, the United Kingdom, and the United States. Through this comparative exercise, the research contrasts India's predominantly decriminalized enforcement model with the hybrid penal frameworks adopted by the United Kingdom and the sector-specific criminal enforcement mechanisms present within the United States.

The comparative methodology facilitates the identification of global best practices relating to regulatory deterrence, proportional sanctions, and institutional accountability. By evaluating these mature legal systems in juxtaposition with India's emerging framework, the study seeks to formulate a balanced, practical, and reform-oriented model capable of strengthening criminal accountability while maintaining regulatory efficiency within India's data governance ecosystem.

1.4 RESEARCH QUESTION

How does India's data protection enforcement framework, particularly in relation to criminal liability, compare with selected international jurisdictions, and what reforms are necessary to develop a balanced, coherent, and effective accountability model within Indian data protection law?

1.5 SCOPE AND LIMITATIONS OF THE STUDY

The present research is confined to a defined geographical, jurisdictional, and conceptual scope in order to effectively fulfil its objective of developing a balanced and practically workable reform model for criminal accountability within Indian data protection law.

From a geographical and jurisdictional perspective, the study primarily examines the Indian legal framework governing data protection, with particular reference to the Digital Personal Data Protection Act, 2023. In order to undertake a meaningful comparative analysis, the scope of the research extends to selected international jurisdictions that represent mature and diverse enforcement models in the field of data protection.

The comparative analysis is specifically limited to the European Union, the United Kingdom, and the United States. In relation to the European Union, the study examines the enforcement architecture established under the General Data Protection Regulation, with particular emphasis on its administrative penalty framework and the criminal enforcement mechanisms retained by individual member states.⁵ With respect to the United Kingdom, the research focuses on the hybrid enforcement model under the Data Protection Act 2018, including the criminal offences preserved under Sections 130 to 173 of the Act. In the context of the United States, the study analyses the sector-specific approach to data protection, particularly the tiered criminal liability mechanisms contained in statutes such as the Health Insurance Portability and Accountability Act of 1996.

Conceptually, the research is strictly confined to the examination of criminal liability, civil and administrative monetary penalties, deterrence theory, standards of fault, and accountability mechanisms as they directly relate to data breaches, unauthorized disclosure, misuse of personal information, and privacy violations.⁶

However, certain limitations must be acknowledged. The study does not undertake a technical or cybersecurity analysis of data breach prevention mechanisms, nor does it examine broader issues relating to cross-border data transfers, competition law, consumer protection, or artificial intelligence regulation, except where such issues directly intersect with criminal accountability in data protection law. Accordingly, the research remains primarily doctrinal and comparative in nature, focusing exclusively on the legal dimensions of enforcement and regulatory accountability.

CHAPTER 2: LITERATURE REVIEW

1. Latham & Watkins LLP, *“India’s Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison”* (2023)

This report by **Latham & Watkins LLP** provides a detailed comparative examination of India’s Digital Personal Data Protection Act, 2023 and the European Union’s General Data Protection Regulation. The report is particularly useful in understanding how India’s newly

⁵ Peter De Cruz, *Comparative Law in a Changing World* 5 (Routledge-Cavendish, 3rd edn., 2007).

⁶ Anthony Ogus, *Regulation: Legal Form and Economic Theory* 67 (Hart Publishing, Oxford, 2004).

enacted framework differs from the globally accepted GDPR model in terms of compliance obligations, enforcement mechanisms, and regulatory design.⁷

The authors identify several important distinctions between the two frameworks. They note that the DPDP Act applies specifically to digital personal data, unlike the GDPR, which adopts a broader scope. The report further highlights that the Indian law follows a predominantly consent-based model for data processing and does not expressly recognize legitimate interest as an independent ground for processing. Another significant observation made in the study relates to data breach reporting, where the DPDP Act requires mandatory notification of every breach, irrespective of the degree of harm or risk involved.

The report also examines India's approach toward cross-border data transfers, the introduction of Consent Managers, and the enhanced compliance obligations imposed upon significant data fiduciaries, including audit requirements and impact assessments. Overall, this report provides valuable insight into the structural and enforcement differences between India's framework and established international models, making it highly relevant for the present study on regulatory accountability and enforcement.

2. Justice B.N. Srikrishna Committee, “*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*” (2018)

The report prepared by the Committee of Experts under **B. N. Srikrishna** serves as one of the most important institutional documents in the development of India's modern data protection framework. It provides the policy and conceptual foundation that later influenced the enactment of the Digital Personal Data Protection Act, 2023. The Committee carefully examined the relationship between individual privacy rights, economic growth in the digital sector, and the legitimate regulatory interests of the State. The report emphasized that an effective data protection framework must strike a balance between protecting personal autonomy and enabling innovation within the digital economy.⁸

A significant contribution of the report lies in its discussion on enforcement mechanisms. Instead of strongly supporting criminal sanctions for data-related violations, the Committee

⁷ Latham & Watkins LLP, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison*, Latham & Watkins LLP (2023), <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-ProtectionAct-2023-vs-the-GDPR-A-Comparison.pdf>.

⁸ Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Elecs. & Info. Tech., Gov't of India, 2018).

largely favoured civil and monetary penalties as a more practical and business-friendly method of ensuring compliance while maintaining accountability. The report also recommended the creation of an independent regulatory authority and emphasized key principles such as data minimization, purpose limitation, and storage limitation.

The Committee's recommendations were informed by international frameworks, including the General Data Protection Regulation, the Convention 108, and the Organisation for Economic Co-operation and Development privacy guidelines. As such, this report remains an essential source for understanding the legislative intent behind India's present data protection regime.

3. Christopher Kuner, *"The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards"* In this study, Christopher Kuner examines the development of data protection law in India and the international influences that shaped its legislative evolution. The work provides an important understanding of how global privacy standards contributed to the emergence of India's domestic data protection framework.

The author explains that international instruments such as the General Data Protection Regulation, the Convention 108, and the privacy guidelines developed by the Organisation for Economic Co-operation and Development played a significant role in influencing Indian policy discussions on data protection.⁹ Kuner also critically evaluates India's early legislative proposals and observes that certain aspects of the proposed framework did not provide sufficiently strong safeguards, particularly in areas involving surveillance, state access to information, and accountability mechanisms.

The study ultimately argues that India should strengthen its legal framework not merely to align with international standards, but to create a robust and socially beneficial privacy regime. This work is particularly relevant for understanding the global normative influences behind India's data protection legislation and its evolving enforcement architecture.

CHAPTER 3: RATIONALE FOR CRIMINAL LIABILITY IN DATA PROTECTION

Modern legal systems use different types of enforcement mechanisms to regulate the misuse of personal data. These mechanisms include civil remedies, administrative penalties, regulatory actions, and criminal sanctions. The choice of a particular enforcement mechanism often depends upon how serious the violation is, what the objectives of the law are, and how strongly

⁹ Christopher Kuner, *The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards*, 33(1) Nat'l L. Sch. India Rev. 69, 69–71 (2021).

the State seeks to protect individual privacy rights. Although many modern data protection frameworks increasingly focus on compliance-based regulation supported by monetary penalties and regulatory oversight, criminal law continues to play an important role in addressing serious and intentional forms of data misuse.

Criminal liability becomes particularly relevant in situations involving deliberate unauthorized access to personal information, unlawful disclosure of confidential records, identity theft, data trafficking, or other intentional acts that cause significant harm to individuals or society. Unlike civil or administrative penalties, criminal sanctions carry stronger legal and social consequences, which makes them an important tool in ensuring accountability and maintaining public trust in digital governance systems.

3.1 DETERRENCE AS A JUSTIFICATION FOR CRIMINAL LIABILITY

One of the most important justifications for introducing criminal liability in data protection law is the principle of deterrence. The possibility of criminal prosecution, along with serious consequences such as imprisonment, substantial financial penalties, and the social stigma associated with a criminal conviction, is generally considered to be a stronger deterrent than civil fines or administrative penalties alone.¹⁰

In the field of data protection, the existence of criminal sanctions may discourage individuals, employees, corporate entities, and other actors from engaging in intentional misconduct such as unauthorized access to databases, illegal sale or transfer of personal information, identity-related fraud, or the deliberate disclosure of confidential data for financial or personal benefit. The fear of criminal punishment therefore plays an important role in preventing serious privacy violations before they occur.

3.2 EXPRESSIVE AND MORAL FUNCTION OF CRIMINAL LAW

Another important justification for criminal liability lies in the expressive function of criminal law. Criminal law does not merely punish wrongful conduct; it also communicates the values that a legal system considers fundamental and deserving of the highest level of protection.

By criminalizing the intentional misuse of personal data, the law sends a clear message to both potential offenders and society at large that personal information is a valuable and protected

¹⁰ Andres von Hirsch et al., CRIMINAL DETERRENCE AND SENTENCE SEVERITY 1-8 (Hart Publ'g 1999).

legal interest.¹¹ It demonstrates that deliberate violations of privacy are not merely regulatory breaches but serious wrongful acts that attract the strongest form of State condemnation.

This expressive function becomes particularly significant in the digital age, where personal information has become deeply connected with individual dignity, autonomy, and informational self-determination.

3.3 PRINCIPLE OF MORAL CULPABILITY AND PROPORTIONAL ENFORCEMENT

Criminal law is generally based on the principle that punishment should be reserved for conduct that is not only harmful but also morally blameworthy. This principle creates important distinctions in the field of data protection, especially between intentional misconduct and accidental or negligent security failures.

Not every data breach necessarily justifies criminal prosecution. Incidents involving technical errors, accidental disclosures, or unintentional compliance failures may be more appropriately addressed through administrative penalties or regulatory corrective measures rather than criminal sanctions.

For this reason, many developed jurisdictions have adopted hybrid enforcement models that match the nature of the sanction with the seriousness of the violation. Under such frameworks, minor regulatory breaches are generally addressed through civil or administrative penalties, while criminal sanctions are reserved for intentional, reckless, fraudulent, or particularly harmful forms of data misuse.¹² This approach helps maintain both fairness and accountability within modern data protection law.

CHAPTER 4: DATA PROTECTION REGIME OF THE EUROPEAN UNION

4.1 Introduction to the EU Data Protection Regime

During the last four decades, the European Union created a sophisticated and internationally acclaimed regime of data protection. Modern regulations of the data protection in the European Union are embodied in Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR), which entered into effect on May 25, 2018, succeeding the former Data Protection

¹¹ Shyamkrishna Balganesh, *Privacy and Personally Identifiable Information on the Internet: Some Thoughts on User Consent and Individual Autonomy*, 9 INDIAN J.L. & TECH. 1, 14-16 (2013).

¹² Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 85-87 (2013).

Directive 95/46/EC. Among GDPR innovations, it is notable that the new regulation established a unified legal framework regulating the processing of personal data in the European Union, involving not only an efficient mechanism of administrative enforcement but also providing for member states the possibility to introduce further criminal sanctions against the infringers of the regime of data protection rights.⁹⁴

4.2 Definition of Personal Data and Sensitive Data

According to GDPR definition, personal data means any information regarding identified or identifiable natural person that includes the following personal data elements such as names, identification numbers, location data, online identifiers or other factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity of the data subject. The categories of data that constitutes sensitive personal data and require additional protection in view of the specific risks to the fundamental rights associated with their processing include the following: genetic, biometric data used to uniquely identify a natural person, data concerning his or her health status, sex life, racial or ethnic origin, religious or philosophical beliefs, political opinions or membership in trade unions.⁹⁵

4.3 Principles of Data Protection under GDPR

Among the most important aspects of GDPR, there is a set of data protection principles applicable to any processing activity performed by data controllers and data processors governed by the GDPR. GDPR data protection principles include the following: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.⁹⁶ These are not just recommendations but legal requirements that must be proven and implemented by organizations in terms of appropriate measures. The principle of accountability requiring proactivity from data controllers in order to ensure data protection requirements is a true novelty of this new system compared to previously existing regimes of data protection, which were mostly characterized by their focus on formal procedures and subsequent reaction to breaches only.

4.4 Enforcement Mechanism under GDPR

GDPR enforcement regime is mainly administrative in its nature. According to the terms of GDPR, each member state shall appoint an independent supervisory authority having the duty to monitor the application of GDPR provisions, handle the claims filed by data subjects, conduct audits, impose sanctions against the defaulting data controllers and data processors.

The supervisory authorities are provided with broad powers to initiate investigations and address cases of non-compliance, including order to cease processing activities and delete data in case of violations. Fines for the data processing violations can amount to €20 million or four percent of the annual worldwide turnover of the controller or processor, depending on what value is higher. This relatively high threshold of penalties was deliberately introduced to make non-compliance much costlier than any gain from misappropriating personal data.

4.5 Criminal Liability under GDPR

While GDPR has a very administratively oriented enforcement framework, criminal liability for data protection offences still plays a crucial role in EU regime of data protection. According to Article 84 of the GDPR, member states are entitled to establish criminal penalties for the offences provided for in GDPR but falling outside the scope of Article 83 dealing with administrative offences. For instance, Germany, Austria, Portugal, and Romania adopted the provisions penalizing intentional data misuse, illegal disclosure of data to third parties, and causing large-scale data breaches. Hence, one can conclude that in the European Union, criminal sanctions and administrative regulation can exist simultaneously with regard to different types of data protection violations.

4.6 Role of the Court of Justice of the European Union

The decisions of the Court of Justice of the European Union were of great importance for developing data protection laws in Europe. As for the landmark case of *Google Spain SL v. Agencia Española de Protección de Datos*, it resulted in recognizing the right to erasure or the right to be forgotten, which entitles people to request the deletion of the personal information that has been lawfully published at first but whose publication now unreasonably harms fundamental rights to privacy and data protection of the respective data subject.¹³ This decision considerably strengthened the protection of data privacy in the Internet and placed substantial responsibilities for compliance with GDPR on internet giants operating in the European Union jurisdiction.

4.7 Landmark Cases in EU Data Protection Law

Another interesting case in point is *Schrems v. Data Protection Commissioner*, where the Court of Justice annulled the Safe Harbour framework that provided the protection of data during the

¹³ *Google Spain SL v. Agencia Española de Protección de Datos*, Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014) (EU).

process of its transferring from the EU to the United States due to lack of sufficient data protection guarantees, particularly taking into consideration the fact that the US intelligence services systematically violate the rights of people by engaging in unauthorized surveillance.¹⁴ This case demonstrated the willingness of the EU to provide for adequate privacy protection for international transfer of personal data and supremacy of data protection over any commercial and geopolitical interests.

Yet another example when data protection issues could be linked to the protection of fundamental constitutional rights is presented in *Digital Rights Ireland Ltd v. Minister for Communications*. The Court of Justice declared the European Union Data Retention Directive unconstitutional, declaring the directive's mandatory requirement of keeping the data about traffic and location generated in course of providing electronically communicated services for a period of up to two years to be disproportional to the pursued goal and therefore violation of the Articles 7 and 8 of the EU Charter of Fundamental Rights securing protection of the fundamental right to privacy and data protection.¹⁵

4.8 Comparative Analysis and Conclusion

Speaking from the point of view of the comparative analysis of the regulatory frameworks discussed in this research paper, the regime of data protection established in the European Union presents a number of interesting points. First of all, the GDPR demonstrates that the combination of an effective administrative enforcement mechanism and severe penalties, an independent supervisory body, and numerous data protection obligations can ensure a proper enforcement of the data protection regulations. On the other hand, the existence of criminal penalties under Article 84 of the GDPR indicates that European regulators believe that civil deterrence is not sufficient for combating all sorts of violations of data protection requirements.¹⁶ This issue is highly relevant in the light of assessing India's emerging data protection framework, in particular, its reliance almost solely on civil penalties under the DPDP Act.

¹⁴ *Schrems v. Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650 (Oct. 6, 2015) (EU).

¹⁵ *Digital Rights Ireland Ltd v. Minister for Communications*, Case C-293/12, ECLI:EU:C:2014:238 (Apr. 8, 2014) (EU).

¹⁶ Christopher Kuner et al., *THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY* 567-72 (Oxford Univ. Press 2020).

Hence, while GDPR heavily relies on substantial penalties, the provision of criminal sanctions for certain types of data protection breaches under Article 84 demonstrates that European regulators understand the limitations of civil deterrence, maintaining criminal penalties as an essential enforcement mechanism.

CHAPTER 5: UNITED KINGDOM: A HYBRID ENFORCEMENT APPROACH

5.1 Evolution of Data Protection Law in the United Kingdom

One of the earliest adopters of data protection legislation, the United Kingdom enacted the first domestic data protection statute, the Data Protection Act 1984. After Brexit, the UK incorporated the essential substance of GDPR through the joint operation of the Data Protection Act 2018 and the UK GDPR – which is an adapted version of the EU Regulation embedded in the UK domestic law. Taken together, the three instruments constitute the current legal framework that regulates the processing of personal data in the United Kingdom.

5.2 Scope and Role of the Data Protection Act 2018

The Data Protection Act 2018 supplements the UK GDPR, dealing with issues of processing that go beyond the reach of the GDPR, such as processing by the competent authorities for the purposes of law enforcement and the processing necessary for the prevention or detection of criminal offenses or breaches of professional ethics.¹⁷ It also specifies matters relating to the processing of personal data by the competent authorities for the purposes of national security or the defence of any member state of the EU or the EEA, and it addresses the issue of intelligence service data handling and sharing. The Act provides that the Information Commissioner's Office is the independent supervisory authority charged with supervising, monitoring, and enforcing compliance. The ICO may investigate, audit, issue guidelines and guidance, and impose sanctions on data controllers and processors in respect of their data processing. Over the years, ICO has proven to be particularly proactive in utilizing its enforcement powers against organizations that do not comply with the statutory requirements by issuing hefty penalty notices.

5.3 Criminal Offences for Misuse of Personal Data

Among the distinguishing characteristics of the UK regime is the retention of criminal offences for the misuse of personal information. According to section 170 of the Data Protection Act

¹⁷ Data Protection Act 2018, c. 12 (UK).

2018, anyone who "knowingly or recklessly" obtains, discloses, or retains personal data without the consent of the controller of the data shall be criminally liable. The inclusion of this criminal provision targets precisely those forms of behaviour that criminal liability is particularly well-suited to punish intentional and reckless abuse of personal information that might arise due to personal gain, improper curiosity, or malice.

5.4 Criminal Liability for Obstruction of Investigation

Furthermore, the Act also contains criminal liability for obstructing an investigation carried out by the Information Commissioner. Such obstructive acts include "altering, defacing, damaging, or destroying information," as well as concealing or disposing of information that the Commissioner may require for the purpose of exercising its regulatory power. The inclusion of such a criminal offense reinforces the efficacy of the regulatory regime because it prevents organizations from attempting to evade regulatory oversight. The provision demonstrates a sensible legislative choice in recognizing that the strength of a regulatory system depends not only on the substantive rules it sets out but also on the ability to properly implement and enforce the system.

5.5 Judicial Developments in Data Protection Law

Several judicial decisions have expanded the remedies available to those whose personal information has been mishandled. In *Google LLC v. Vidal-Hall*, the Court of Appeal recognized the tort of misuse of private information as an actionable wrong that can result in compensatory relief even if no direct pecuniary loss has been suffered.¹⁸ This decision was significant both in terms of its doctrinal implications and practical effects because it allowed victims of the misuse of personal data to obtain appropriate compensation for the distress caused, regardless of whether they incurred a pecuniary loss.

5.6 Representative Actions and the *Lloyd v. Google* Case

In the landmark UK Supreme Court decision *Lloyd v. Google LLC* issued in 2021, the question arose whether representative proceedings on behalf of large groups of victims of systemic privacy violations could be brought, where it was not possible to prove that individual plaintiffs were harmed in a way different from being victims of unauthorized use of personal data.¹⁹ The Court denied a representative action in that case owing to the lack of evidence of a single type

¹⁸ *Google LLC v. Vidal-Hall*, [2015] EWCA (Civ) 311 (Eng.).

¹⁹ *Lloyd v. Google LLC*, [2021] UKSC 50 (Eng.).

of loss suffered by each and every group member. Nevertheless, the decision raised an important debate concerning whether individual actions are sufficient to adequately address large-scale data misuse by global companies. The UK approach demonstrates a hybrid enforcement system, combining administrative regulation with criminal liability and tailoring the latter according to the type and gravity of the violation – an important structural aspect to consider when analysing India's shift towards civil penalties for data violations.

CHAPTER 6: THE UNITED STATES: SECTORAL REGULATION AND TARGETED CRIMINAL LIABILITY

6.1 Evolution of the American Data Protection Model

In contrast to the European Union's harmonised and comprehensive approach to data protection, the United States has historically adopted a sector-specific and decentralised regulatory model. Instead of enacting a single federal statute comparable to the General Data Protection Regulation (GDPR), the United States Congress has developed a complex framework of federal and state laws that regulate different categories of personal data depending upon the sector involved, the nature of the data subject, and the entity engaged in processing.²⁰ This approach reflects broader characteristics of American regulatory philosophy, including a preference for targeted legislative intervention, strong commercial influence over privacy policymaking, and the constitutional significance of First Amendment values in matters involving information and communication.

6.2 Sector-Specific Federal Privacy Legislation

Among the most significant federal statutes governing personal data is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA regulates the handling of protected health information by healthcare providers, health plans, healthcare clearinghouses, and their business associates.²¹ The statute establishes detailed privacy and security standards designed to preserve the confidentiality, integrity, and availability of sensitive medical information. One of the most notable features of HIPAA is its graduated penalty structure, which combines civil and criminal liability based on the degree of culpability involved. Minor violations may attract administrative penalties, while more serious violations committed under

²⁰ Paul M. Schwartz & William M. Treanor, *INFORMATION PRIVACY: STATUTES, REGULATIONS, AND CASES* 1-12 (5th ed., Found. Press 2021).

²¹ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 ¹¹³ Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338.

false pretences or with intent to sell, transfer, or exploit health information for personal or commercial gain may result in substantial fines and imprisonment. This proportional enforcement model demonstrates a carefully calibrated approach to deterrence.

Another important federal statute is the Gramm-Leach-Bliley Act (GLBA), which regulates the collection, use, and disclosure of non-public financial information by banking institutions and financial service providers. The Act requires financial institutions to implement comprehensive safeguard programmes to ensure the security and confidentiality of consumer financial data, while also mandating privacy notices and providing consumers with opt-out rights regarding data sharing practices.

Similarly, the Children's Online Privacy Protection Act of 1998 (COPPA) provides targeted protection for personal information collected online from children under the age of thirteen. The Act requires verifiable parental consent before such data may be collected and grants enforcement authority to the Federal Trade Commission (FTC).²²

6.3 Criminal Liability Under the Computer Fraud and Abuse Act

The principal federal criminal statute addressing unauthorised access to computer systems and misuse of digital information is the Computer Fraud and Abuse Act of 1986 (CFAA). The CFAA criminalises intentional unauthorised access to protected computer systems, as well as the unlawful obtaining, transmission, or use of information stored within such systems.²³ Over the years, the statute has been widely applied in criminal prosecutions involving large-scale hacking operations, mass data theft, misuse of digital credentials, and intentional disruption of computer networks.

Despite its importance, the CFAA has attracted significant criticism due to its broad wording, which has occasionally raised concerns regarding over-criminalisation. The scope of criminal liability under the statute was clarified by the United States Supreme Court in *Van Buren v. United States*, where the Court held that an individual does not violate the CFAA merely by accessing information for an improper purpose, provided that the person was otherwise authorised to access the computer system. This decision reflected growing judicial concern

²² Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6505

²³ Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

regarding proportionality in digital criminal law and the need for clear statutory boundaries defining authorised access.

6.4 The Role of the Federal Trade Commission

The Federal Trade Commission occupies a unique position in the governance of data privacy in the United States. Acting under Section 5 of the Federal Trade Commission Act, the FTC possesses authority to prohibit unfair or deceptive trade practices affecting commerce.²⁴ Through expansive interpretation of this power, the Commission has treated failures to comply with publicly stated privacy policies and inadequate cybersecurity practices as deceptive or unfair conduct.

By means of consent decrees, public enforcement actions, and substantial civil monetary penalties, the FTC has emerged as a highly influential regulator in the American privacy landscape. However, its authority to impose penalties for first-time violations remains limited in the absence of prior rule violations, which some scholars argue reduces its deterrent capacity when compared to the stronger enforcement powers available under the GDPR framework.

6.5 State-Level Innovation: The California Model

At the state level, California has emerged as the leading jurisdiction in privacy regulation through the enactment of the California Consumer Privacy Act of 2018 (CCPA), subsequently strengthened by the California Privacy Rights Act of 2020. These laws created the California Privacy Protection Agency and granted residents significant rights over their personal data, including rights of access, deletion, correction, and the ability to opt out of certain forms of data sale.

California's legislative leadership demonstrates growing political momentum toward stronger privacy protections in the United States, while simultaneously highlighting the continued absence of consensus on a unified federal privacy framework.

CHAPTER 7: CONCLUSION AND SUGGESTIONS

The comparative and doctrinal analysis undertaken in this research produces several significant findings regarding the position of criminal accountability within India's emerging data protection framework. These findings directly address the research objectives and the central

²⁴ Federal Trade Commission Act of 1914, 15 U.S.C. §

research question, namely, whether India's present enforcement framework provides a balanced, coherent, and effective accountability model when compared with mature international jurisdictions such as the European Union, the United Kingdom, and the United States.

7.1 Conclusion

This research concludes that India's current data protection enforcement framework represents a significant departure from established international regulatory practice. While the Digital Personal Data Protection Act, 2023 introduces an important administrative framework for data governance, its complete reliance on civil monetary penalties creates identifiable weaknesses in deterrence, individual accountability, and normative legitimacy.

The comparative study of the European Union, the United Kingdom, and the United States demonstrates that mature regulatory systems have consistently adopted hybrid enforcement models in which administrative penalties address routine compliance failures, while criminal sanctions remain available for deliberate, reckless, or seriously harmful violations. India's decision to abandon criminal accountability entirely is not supported by comparative evidence, constitutional reasoning, or legislative policy analysis. The findings of this research therefore confirm that the present framework does not yet provide a fully balanced or coherent model of accountability.

7.2 Suggestions and Recommendations

Based on the findings of this research, the reform proposals set out in this section seek to address three interrelated structural deficiencies within India's current data protection framework: first, the complete absence of criminal accountability for deliberate and harmful data-related misconduct; second, the inconsistency of fault standards across overlapping statutory frameworks; and third, the institutional weaknesses that may undermine effective enforcement irrespective of the substantive legal standards adopted. The comparative analysis undertaken in this study demonstrates that these deficiencies are neither inevitable nor conceptually difficult to address. Mature regulatory systems have developed workable models that balance administrative compliance with targeted criminal accountability, institutional independence, and internal governance obligations. India's evolving framework can be strengthened through carefully designed and context-sensitive reforms rather than wholesale legislative replacement.

7.2.1 Introduction of Targeted Criminal Offences

The first and most significant reform recommended by this research is the introduction of a limited category of criminal offences aimed specifically at deliberate, reckless, and seriously harmful forms of data-related misconduct. Criminal liability should not extend to ordinary compliance failures, technical breaches, or negligent procedural lapses. Rather, it should be reserved for conduct that involves conscious wrongdoing, abuse of trust, or intentional exploitation of personal information.

(a) Intentional Re-identification of Anonymised Data

The first proposed offence is the intentional re-identification of de-identified or anonymised personal data without lawful authority. Re-identification is not an accidental compliance failure but a deliberate technical act designed to defeat privacy protections that anonymisation is specifically intended to provide. Such conduct undermines one of the most important mechanisms through which organizations reduce privacy risk in data processing.

The Justice B.N. Srikrishna Committee, in its 2018 report, expressly recommended criminal liability for this conduct, and the findings of this research strongly support that recommendation. It is therefore proposed that intentional re-identification be criminalised with a punishment of imprisonment extending up to five years, along with the possibility of a concurrent monetary fine.

(b) Knowing or Reckless Unauthorised Disclosure of Personal Data

The second proposed offence concerns the knowing or reckless unauthorised disclosure of personal data by individuals who hold such data in positions of trust, confidence, or official authority. This includes employees, public officials, compliance officers, contractors, healthcare personnel, financial service employees, and any other individuals who gain access to personal data by virtue of professional or fiduciary responsibility.

This proposal draws directly from Section 170 of the United Kingdom's Data Protection Act, 2018. The inclusion of recklessness alongside intention is particularly important. It ensures that liability extends not only to those who knowingly disclose personal information unlawfully, but also to those who consciously disregard a substantial and unjustifiable risk that their conduct lacks legal authorisation. Such a formulation prevents individuals from avoiding accountability by claiming ignorance where that ignorance itself was the result of deliberate indifference.

7.2.2 Corporate and Individual Criminal Liability

The effectiveness of criminal sanctions depends not only upon identifying prohibited conduct but also upon ensuring that liability reaches those individuals who actually control organisational decision-making.

Accordingly, corporate criminal liability for the proposed offences should be attributed through the identification doctrine, under which the mental state of the corporation's "directing mind and will" is treated as the mental state of the corporate entity itself. This principle has already been recognised by the Supreme Court of India in *Standard Chartered Bank v. Directorate of Enforcement*.

At the same time, the amended framework should impose direct personal criminal liability upon directors, senior executives, compliance officers, and managerial personnel who personally authorise, facilitate, conceal, or knowingly permit the commission of any of the specified offences.

This reform directly addresses the accountability gap identified in the DPDP Act, under which corporate entities may be fined while the individuals responsible for unlawful decisions face no personal legal consequences.

7.2.3 Harmonisation of Statutory Fault Standards

A further reform necessary for doctrinal coherence is the resolution of overlapping statutory provisions relating to data misuse under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023.

This research recommends the formal repeal or integration of Sections 72 and 72A of the Information Technology Act to eliminate statutory duplication and uncertainty regarding applicable fault standards. A unified legislative framework should clearly distinguish between negligence, recklessness, and intentional misconduct, with sanctions proportionately calibrated to each level of culpability.

Such harmonisation would enhance legal certainty, improve prosecutorial consistency, and align Indian law with comparative international practice.

7.2.4 Review of State Exemptions and Constitutional Oversight

Finally, the broad exemptions granted under Section 17 of the DPDP Act should be subjected to independent proportionality review. Given the constitutional significance of informational

privacy following *Justice K.S. Puttaswamy v. Union of India*, exemptions affecting state surveillance, public administration, or law enforcement should not operate without meaningful oversight.

A statutory mechanism should therefore be introduced requiring periodic independent review of such exemptions against the constitutional standards of legality, necessity, and proportionality.

A review of the legislative evolution of digital governance in India reveals a recurring pattern: each statutory reform has addressed important deficiencies while simultaneously creating new regulatory challenges. The Information Technology Act, 2000 introduced India's first digital governance framework but approached personal data primarily through a commercial lens. The 2008 amendments introduced criminal liability but relied upon fault standards that proved difficult to apply in rapidly evolving digital environments. The Digital Personal Data Protection Act, 2023 marks an important transition toward a rights-based framework but simultaneously eliminates individual criminal accountability and creates structural concerns regarding institutional independence.

What distinguishes the accountability gap created by the DPDP Act is that it was not unforeseen. The Srikrishna Committee identified the need for criminal sanctions. Comparative international models preserving criminal accountability were readily available. Academic commentary and civil society submissions repeatedly highlighted the risks of complete decriminalisation. The present gap is therefore not a product of legislative ignorance, but of legislative choice. However, legislative choices are not immutable. Since the DPDP framework remains in its early stages of implementation, there remains a significant opportunity to address these structural weaknesses before they become entrenched through years of inadequate enforcement.

The path forward does not require replacing the existing framework. It requires targeted and carefully calibrated amendments—reintroducing criminal accountability for deliberate violations, harmonising fault standards, strengthening institutional independence, and ensuring constitutional oversight. Comparative experience demonstrates that these reforms are both legally achievable and practically necessary for the development of a coherent and effective Indian data protection regime.