VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# DATA HARVESTING AS AN ECONOMIC CRIME: INVESTIGATING THE MISUSE OF PERSONAL DATA BY LOAN APPS AND FINTECH OPERATORS

- Pravin Raj[1] & Vaishali T

## ABSTRACT:

The rapid expansion of digital lending and financial technology (FinTech) platforms in India has significantly enhanced access to credit and accelerated financial inclusion. However, this growth has also fostered a parallel ecosystem of excessive data harvesting, unauthorized data sharing, and coercive exploitation of personal and device-level information.

This paper conceptualizes such data harvesting practices by loan applications and FinTech operators as a form of economic crime, highlighting how personal data is collected beyond necessity, monetized, and weaponized to enable predatory lending, harassment, extortion, and other abusive practices.

By enquiring and by passing in empirical evidence from regulatory reports, enforcement actions, and documented case studies, the study critically evaluates the adequacy of India's existing legal framework, particularly the Information Technology Act, 2000, the Reserve Bank of India's digital lending regulations, and the Digital Personal Data Protection Act, 2023. The analysis reveals regulatory fragmentation, enforcement gaps, and compliance challenges that continue to facilitate the misuse of personal data despite an evolving statutory regime.

## Aims and Objectives of the Study

[1] LLM, Cyber Space Law And Justice Soel – School of Excellence in Law

The present study is undertaken with the following aims and objectives:

1. **To conceptualise data harvesting as an economic crime** by analysing how the misuse of personal data by loan apps results in economic exploitation, unfair enrichment, and systemic market harm.
2. **To examine the operational practices of loan apps and FinTech operators**with specific focus on excessive data collection, coercive consent mechanisms, algorithmic profiling, and abusive recovery methods.
3. **To analyse the adequacy of the existing Indian legal framework**, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, RBI digital lending guidelines, and general criminal law, in addressing data-driven economic offences.
4. **To identify enforcement challenges and regulatory gaps** arising from technological complexity, jurisdictional issues, and regulatory fragmentation. To propose legal and policy reforms aimed at recognising, preventing, and prosecuting exploitative data harvesting as an economic crime.

## INTRODUCTION

Digital lending platforms and mobile-based loan applications have emerged as defining features of contemporary financial markets, reshaping access to credit through big data analytics, alternative credit scoring, and instant digital onboarding. In India, this rapid growth has been driven by widespread smartphone penetration, robust digital identity infrastructure, and interoperable payment systems, positioning FinTech as a key instrument of financial inclusion. However, the increasing dependence on digital systems has simultaneously intensified the risks of data theft, unauthorized access, and misuse of personal information. In India, such threats are primarily governed by the Information Technology Act, 2000, which establishes the foundational legal framework for addressing cybercrimes, including data theft and unauthorized disclosure. This article provides an in-depth analysis of data theft under the IT Act, examining its legal provisions, penalties, notable judicial and regulatory cases, and preventive mechanisms for safeguarding sensitive information.

The study further situates these concerns within India’s broader digital transformation, marked by its status as the world’s second-largest internet market and an unprecedented scale of data generation. While the Digital Personal Data Protection Act, 2023 has emerged as a cornerstone of India’s data governance regime, it also raises complex questions regarding individual privacy and state power. The expansion of government surveillance capabilities through mechanisms such as the Central Monitoring System and Network Traffic Analysis underscores the growing tension between national security imperatives and civil liberties. Drawing on constitutional principles affirmed in the landmark Justice K.S. Puttaswamy v. Union of India (2017) judgment, this paper critically examines whether India’s evolving legal framework adequately balances innovation, security, and the fundamental right to privacy in an increasingly data-driven economy.

## 1. Conceptual Framework: Data Harvesting as Economic Crime

The rapid digitisation of financial services has transformed personal data into one of the most valuable economic resources of the modern economy. In the context of digital lending and FinTech operations, personal data is no longer merely informational but functions as a strategic economic asset that enables profit maximisation, risk reduction, and behavioural control. This objective seeks to conceptualise **data harvesting by loan apps as an economic crime**, rather than viewing it narrowly as a privacy or regulatory violation. By analysing the mechanisms through which personal data is misused, this study demonstrates how such practices lead to **economic exploitation of borrowers, unfair enrichment of digital lenders, and systemic harm to market integrity**.

1.Mr. Neeraj Soni, Policy & Advocacy, CyberPeace.org

### Data as an Economic Resource and Instrument of Power

Traditionally, economic crimes have been associated with tangible assets such as money, securities, or property. However, in the digital economy, **personal data performs an equivalent economic function**. Loan apps rely heavily on large-scale data extraction to fuel alternative credit scoring models, automate decision-making, and enhance recovery efficiency. Data harvested from borrowers—such as contact lists, location data, call logs, and behavioural metadata—enables lenders to predict repayment behaviour, reduce transaction costs, and exert pressure during recovery.

When such data is collected lawfully, proportionately, and with informed consent, it may be justified as part of legitimate business operations. However, when data is extracted through **deceptive interfaces, or excessive permissions unrelated to credit assessment**, it becomes a tool of economic exploitation. The borrower, often in a position of financial vulnerability, is compelled to surrender valuable personal data in exchange for short-term credit. This imbalance mirrors classical patterns of economic crime, where power asymmetry is exploited to extract value unfairly.

### Economic Exploitation Through Coercive Data Practices

Economic exploitation occurs when one party derives disproportionate benefit by taking advantage of another's vulnerability. In the digital lending ecosystem, borrowers—particularly low-income individuals, gig workers, students, and first-time credit users—often lack bargaining power, financial literacy, and meaningful alternatives. Loan apps capitalise on this vulnerability by conditioning access to credit on blanket data permissions.

The misuse of harvested data extends beyond credit assessment into recovery and enforcement practices. Access to contact lists and social networks allows lenders or their agents to engage in **public shaming, harassment, and intimidation**, thereby transforming personal data into an enforcement mechanism. Such practices impose significant economic costs on borrowers, including loss of employment, reputational damage, social exclusion, and mental health consequences that impair earning capacity. These harms are not incidental but are structurally embedded in data-driven recovery models, underscoring the exploitative nature of such practices.

This form of exploitation is analogous to **cheating or criminal breach of trust**, where consent is obtained through misrepresentation and the entrusted asset (data) is misused for ulterior purposes. The borrower's data is effectively weaponised to extract ~~repayment or compliance, even when such me~~thods violate legal and ethical norms.

[2] **Shoshana Zuboff**, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)

[3] **World Economic Forum**, *Personal Data: The Emergence of a New Asset Class* (WEF Report, 2011)

## Unfair Enrichment and Monetisation of Illegally Harvested Data

A core element of economic crime is **unjust or unfair enrichment**—the accumulation of wealth through unlawful or unethical means. Data harvesting enables FinTech operators to generate value far exceeding the immediate loan transaction. Personal data is monetised through profiling, analytics, third-party sharing, and targeted marketing. In some cases, data is transferred to external recovery agents or analytics firms, creating secondary and tertiary revenue streams.

This enrichment is unfair because it is derived from data obtained without genuine, informed consent and often in violation of statutory safeguards. Borrowers receive no share in the economic value generated from their data, despite bearing the risks of misuse, breaches, and harassment. The asymmetry between who bears the cost and who captures the benefit is a defining characteristic of economic crime.

Moreover, unlawful data harvesting allows digital lenders to **externalise costs**. By relying on data-driven coercion instead of lawful recovery mechanisms, loan apps reduce operational expenses while shifting the social and psychological costs onto borrowers and society. Such practices distort the cost-benefit structure of lending and incentivise aggressive, unethical business models.

### Systemic Market Harm and Distortion of Competition

Beyond individual exploitation, data harvesting by loan apps produces **systemic harm to the financial market**. Ethical and compliant lenders who adhere to data minimisation and fair recovery practices face higher compliance costs. In contrast, operators engaging in exploitative data harvesting gain a competitive advantage by reducing risk and enforcement costs through unlawful means. This creates a **race to the bottom**, where unethical practices become normalised.

Market trust is a foundational element of financial systems. Widespread reports of harassment, data misuse, and coercive recovery erode public confidence in digital lending, discouraging responsible financial inclusion. This undermines regulatory objectives and damages the long-term sustainability of FinTech innovation.

Such practices contribute to regulatory arbitrage, shadow lending, and informalisation of digital finance. When data misuse goes unchecked, it weakens the rule of law in financial markets and necessitates heavy-handed regulatory interventions that may stifle genuine innovation.

[4] **Julie E. Cohen**, "Law for the Platform Economy," *UC Davis Law Review*, Vol. 51 (2017)

[5] **OECD**, *Consumer Policy and Fraud: Economic Harms from Data Misuse* (2018)

[6] **Supreme Court of India**, *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

### Reframing Data Misuse Within Economic Crime Theory

Conceptualising data harvesting as an economic crime enables a more robust legal and regulatory response. Economic crime theory recognises that harm may be **diffuse, systemic, and long-term**, rather than immediate and individualised. Data-driven exploitation fits squarely within this framework, as its harms accumulate across large populations and over time.

Viewing data harvesting through the lens of economic crime shifts the focus from mere compliance failures to **culpable conduct deserving of deterrent sanctions**. It supports the argument for criminal liability in cases of aggravated misuse, particularly where data exploitation leads to severe economic or social harm. This reframing also strengthens enforcement by justifying coordinated action by financial regulators, data protection authorities, and criminal justice agencies

### 2. To examine the operational practices of loan apps and FinTech operators

The digital lending ecosystem is fundamentally driven by technology-enabled operational practices that distinguish loan apps and FinTech operators from traditional financial institutions. While these innovations promise efficiency and financial inclusion, they also introduce new risks associated with the misuse of personal data and algorithmic power. This objective seeks to critically examine the **operational practices of loan apps and FinTech operators**, with particular emphasis on **excessive data collection, coercive consent mechanisms, algorithmic profiling, and abusive recovery methods**. By analysing these practices, the study highlights how operational design choices contribute to economic exploitation and legal violations within the digital lending framework.

### Excessive and Disproportionate Data Collection

One of the most significant operational practices of loan apps is the collection of extensive personal data far beyond what is necessary for credit assessment. Unlike traditional lenders, who rely primarily on financial documents and credit histories, loan apps often seek access to a wide range of device-level and behavioural data. This includes contact lists, call logs, SMS records, photographs, location data, device identifiers, and application usage patterns.

Excessive data collection also creates significant risks of misuse, unauthorised sharing, and data breaches. The aggregation of sensitive data enables loan apps to construct detailed personal profiles that can be exploited for economic gain. From a legal standpoint, such practices undermine the validity of consent and expose FinTech operators to liability under data protection and cyber laws.

[7] **RBI**, *Report of the Working Group on Digital Lending* (2021)

[8] **Supreme Court of India**, *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637.

Disproportionate data collection represents the **systematic extraction of value** from borrowers under conditions of informational and bargaining asymmetry.

### Coercive Consent Mechanisms and Dark Patterns

Consent forms the legal foundation for lawful data processing. However, in the digital lending context, consent is often obtained through **coercive and deceptive mechanisms** that undermine its voluntariness and informed nature. Loan apps commonly employ "take-it-or-leave-it" models, where access to urgently needed credit is conditional upon granting sweeping data permissions.

Privacy policies and terms of service are frequently lengthy, complex, and written in technical language that an average user cannot reasonably be expected to understand. Pre-ticked boxes, bundled consent for multiple purposes, and vague disclosures regarding third-party data sharing further erode meaningful choice. These design strategies, often referred to as **dark patterns**, manipulate user behaviour and exploit cognitive biases.

The coercive nature of consent is particularly problematic given the socio-economic profile of many borrowers. Individuals facing financial distress may feel compelled to accept intrusive terms without genuine understanding or alternatives. Legally, such consent may be considered invalid, as it is neither free nor informed. Economically, it enables FinTech operators to legitimise exploitative practices while shifting responsibility onto users.

By normalising coerced consent, loan apps convert a formal legal requirement into a procedural façade. This practice highlights the gap between doctrinal consent standards and operational realities, reinforcing the argument that regulatory oversight alone may be insufficient without stricter enforcement and accountability mechanisms.

### Algorithmic Profiling and Automated Decision-Making

Algorithmic profiling lies at the core of digital lending operations. Loan apps rely on automated systems to assess creditworthiness, determine loan terms, and trigger recovery actions. These algorithms process vast quantities of personal and behavioural data to generate risk scores and predictive outcomes.

[9] **Mathur et al.**, "Dark Patterns at Scale," *Proceedings of the ACM on Human-Computer Interaction* (2019)

[10] **Supreme Court of India**, *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1

[11] **GDPR**, Article 22 and Recital 71

Sandra Wachter, Brent Mittelstadt & Luciano Floridi

[12] **FTC (USA)**, *Bringing Dark Patterns to Light* (Staff Report, 2022).

While algorithmic decision-making enhances efficiency, it raises serious concerns regarding **transparency, fairness, and accountability**. Borrowers are rarely informed about the criteria used to evaluate them, nor do they have access to meaningful explanations for adverse decisions. This opacity prevents users from challenging errors, biases, or discriminatory outcomes embedded in algorithmic models.

From a legal perspective, unchecked algorithmic profiling undermines principles of natural justice and due process. From an economic standpoint, it enables FinTech operators to **systematically categorise and control borrowers**, extracting value while minimising institutional risk. When profiling leads to discriminatory or arbitrary outcomes, it exacerbates social inequality and erodes trust in digital financial systems.

### Abusive and Data-Driven Recovery Methods

Perhaps the most visible manifestation of exploitative operational practices is the use of **abusive recovery methods** facilitated by harvested data. Access to borrowers' contacts, photographs, and social networks allows loan apps and their agents to exert intense social and psychological pressure during recovery.

Documented practices include contacting family members, employers, and acquaintances; disseminating defamatory messages; and using threats or humiliation to compel repayment. In some cases, personal photographs have been manipulated or shared to shame borrowers publicly. These actions cause severe reputational harm, loss of employment, and emotional distress, translating into tangible economic consequences.

Such recovery methods violate principles of fair debt collection and, in many cases, attract criminal liability under general penal law. The use of data as a recovery weapon underscores how operational practices transform personal information into a mechanism of economic coercion.

abusive recovery methods represent the culmination of data-driven exploitation. The initial act of excessive data collection enables subsequent coercion, creating a closed loop of exploitation that benefits the lender while devastating the borrower.

### Interconnectedness of Operational Practices

Excessive data collection, coercive consent, algorithmic profiling, and abusive recovery methods are not isolated practices but **interconnected components of a single operational model**.

[13] **Reserve Bank of India (RBI)**, *Guidelines on Digital Lending* (2022).

[14] **RBI**, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (2021)

Each stage reinforces the next, creating a system in which personal data is extracted, processed, and deployed to maximise economic advantage. Understanding this interconnectedness is crucial for effective regulation and accountability

### 3.To analyse the adequacy of the existing Indian legal framework.

### Analysing the Adequacy of the Indian Legal Framework in Addressing Data-Driven Economic Offences

The rapid expansion of digital lending and FinTech operations has posed significant challenges to India's existing legal and regulatory architecture. Data-driven economic offences, particularly those arising from exploitative data harvesting by loan apps, cut across multiple legal domains, including cyber law, data protection, financial regulation, and criminal law. This objective seeks to critically analyse the **adequacy of the existing Indian legal framework**—comprising the **Information Technology Act, 2000**, the **Digital Personal Data Protection Act, 2023**, **Reserve Bank of India (RBI) digital lending guidelines**, and **general criminal law provisions**—in addressing such offences. The analysis reveals that while India has made notable strides in recognising and regulating data misuse, significant gaps remain in enforcement, coordination, and conceptualisation of data-driven harms as economic crimes.

### The Information Technology Act, 2000: Foundational but Limited

The Information Technology Act, 2000 (IT Act) constitutes the primary statutory framework governing cyber offences in India. Enacted at a time when digital finance was in its nascent stages, the Act focuses largely on unauthorised access, data damage, and computer-related offences. Provisions such as Sections 43 and 66 impose civil and criminal liability for unauthorised access to computer systems, data theft, and related acts. Section 72A addresses the disclosure of personal information in breach of lawful contract.

While these provisions are relevant to instances of data misuse by loan apps, their applicability is **indirect and fragmented**. The IT Act does not explicitly address excessive or disproportionate data collection undertaken with ostensible consent. As a result, practices such as coercive permission-seeking or purpose-deviant data usage often fall into legal grey areas. Moreover, enforcement under the IT Act has traditionally focused on hacking and cyber intrusion rather than systemic exploitation of lawfully accessed data.

From the perspective of economic crime, the IT Act lacks a clear framework to address **value extraction through data exploitation**. It treats data misuse primarily as a technical or contractual violation rather than a form of economic wrongdoing with widespread societal impact. Consequently, while the Act provides a foundational layer of protection, it is insufficient to address the complex, data-driven business models employed by modern FinTech operators.

### Digital Personal Data Protection Act, 2023: A Rights-Based Shift

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant evolution in India’s approach to data governance. The Act introduces principles such as lawful purpose, data minimisation, consent, and accountability,

**15.Justice B.N. Srikrishna Committee**, *Report of the Committee of Experts on a Data Protection Framework for India* (2018).

**16.Supreme Court of India**, *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1. *(Recognises informational privacy and implicitly critiques the IT Act’s limited safeguards.)*

**17.Supreme Court of India**, *Shreya Singhal v. Union of India* (2015) 5 SCC 1. *(Demonstrates the IT Act’s focus on speech and intermediaries rather than economic data misuse.)*

reflecting global best practices. It recognises individuals as “data principals” and imposes obligations on “data fiduciaries” to process personal data responsibly.

In the context of loan apps, the DPDP Act directly addresses many problematic practices, including excessive data collection and non-transparent data sharing. The requirement of **free, informed, specific, and unambiguous consent** challenges the legitimacy of coercive consent mechanisms commonly used in digital lending. Penalties for non-compliance are substantial, signalling legislative intent to deter misuse.

However, the DPDP Act’s effectiveness in addressing data-driven economic offences is constrained by several factors. First, the Act is primarily **regulatory and civil in nature**, focusing on compliance and penalties rather than criminal culpability. Second, it grants significant exemptions to the State and allows delegated rule-making, which may dilute protections in practice. Third, the absence of a fully operational and independent Data Protection Board raises concerns about enforcement capacity.

Crucially, the DPDP Act does not explicitly frame data misuse as an economic offence. While it recognises harm and imposes penalties, it stops short of integrating data exploitation into the broader criminal justice framework. As a result, severe cases of economic harm caused by data misuse may not attract proportionate sanctions.

### RBI Digital Lending Guidelines: Sector-Specific Oversight

Recognising the unique risks posed by digital lending, the Reserve Bank of India has issued a series of guidelines aimed at regulating loan apps and FinTech intermediaries. These guidelines emphasise transparency, fair practices, and data privacy. Regulated entities are required to ensure that loan apps collect only necessary data, obtain explicit consent, and refrain from engaging in coercive recovery practices.

The RBI’s approach reflects an understanding of the systemic risks posed by data misuse in financial markets. By placing responsibility on regulated lenders to oversee their FinTech partners, the guidelines seek to prevent regulatory arbitrage. The requirement of auditability and grievance redress mechanisms further strengthens consumer protection.

Nevertheless, RBI guidelines suffer from **structural limitations**. They apply primarily to regulated entities and rely on indirect oversight of FinTech operators. Many loan apps operate in quasi-formal or informal arrangements, complicating enforcement. Additionally, RBI’s mandate is prudential rather than penal, limiting its ability to impose criminal sanctions for egregious misconduct.

Thus, RBI framework addresses symptoms rather than root causes. It focuses on compliance and risk management without explicitly recognising data misuse as a form of economic exploitation warranting criminal investigation.

### General Criminal Law: Fragmented and Reactive

General criminal law provisions, now embodied in the Bharatiya Nyaya Sanhita, provide remedies for acts such as cheating, criminal intimidation, defamation, and breach of trust. In cases of extreme harassment or coercion by loan apps, these provisions have been invoked to prosecute recovery agents and app operators.

While criminal law offers a powerful deterrent, its application to data-driven offences is often **reactive and case-specific**. Prosecution typically occurs only after severe harm, such as suicide or public scandal, has already taken place. Moreover, the absence of explicit offences relating to data exploitation creates evidentiary and interpretive challenges.

Criminal law also struggles to address corporate and algorithmic culpability. Establishing mens rea in complex FinTech operations, where decisions are automated and responsibilities diffused, remains a significant hurdle. Consequently, criminal law alone cannot serve as a comprehensive solution.

### Overall Assessment of Adequacy

The existing Indian legal framework reflects a **piecemeal approach** to data-driven economic offences. Each component addresses certain aspects of the problem, yet none offers a holistic solution. The IT Act provides technical safeguards, the DPDP

Act establishes rights and obligations, RBI guidelines offer sector-specific oversight, and criminal law addresses extreme misconduct. However, the absence of conceptual integration limits their collective effectiveness.

Data-driven economic offences require a legal response that recognises data as an economic asset and misuse as a form of financial wrongdoing. Without such recognition, enforcement remains fragmented, penalties may lack deterrent value, and victims may struggle to obtain meaningful redress

**4.To identify enforcement challenges and regulatory gaps** arising from technological complexity, jurisdictional issues, and regulatory fragmentation.To propose legal and policy reforms aimed at recognising, preventing, and prosecuting exploitative data harvesting as an economic crime

**Identifying Enforcement Challenges and Regulatory Gaps in Data-Driven Economic Offences**

The regulation of exploitative data harvesting by loan apps and FinTech operators presents complex enforcement challenges that extend beyond conventional legal paradigms. While India has developed multiple statutory and regulatory mechanisms to address data misuse, their effectiveness is constrained by **technological complexity, jurisdictional limitations, and regulatory fragmentation**. This objective seeks to identify and analyse these enforcement challenges and regulatory gaps, demonstrating how they undermine accountability and enable data-driven economic offences to persist.

[18] **Indian Penal Code, 1860**, Sections 383–389 (Extortion), 415–420 (Cheating), 503–507 (Criminal Intimidation).

[19] **Code of Criminal Procedure, 1973**, Sections 154, 156 and 173.

[20] **Supreme Court of India**, *State of Haryana v. Bhajan Lal* 1992 Supp (1) SCC 335.

[21] **Supreme Court of India**, *G. Sagar Suri v. State of U.P.* (2000) 2 SCC 636.

### Technological Complexity and Algorithmic Opacity

One of the foremost challenges in enforcing laws against exploitative data harvesting arises from the **technological sophistication of FinTech operations**. Loan apps rely on proprietary algorithms, machine-learning models, and automated decision-making systems that process vast amounts of personal data. These systems are often opaque, even to regulators, due to claims of trade secrecy and intellectual property protection.

Algorithmic opacity creates significant evidentiary barriers. Investigating authorities may struggle to determine how specific data points influence credit decisions, recovery strategies, or profiling outcomes. This lack of transparency makes it difficult to establish causation, intent, or culpability—elements essential for criminal prosecution. Moreover, automated systems distribute responsibility across developers, operators, and third-party service providers, complicating attribution of liability.

Technological complexity also enables **regulatory evasion**. Data may be encrypted, anonymised, or routed through multiple servers, obscuring audit trails. Such practices hinder forensic analysis and delay enforcement actions, allowing exploitative models to operate with minimal oversight.

22.**Parliamentary Standing Committee on Information Technology**, *Report on Citizens' Data Security and Privacy* (2021).
23.**Reserve Bank of India**, *Report of the Working Group on Digital Lending* (2021).
26.**Competition Commission of India v. Google LLC**, CCI Order (2022).
27.**National Crime Records Bureau (NCRB)**, *Crime in India* Reports (recent editions).

### Jurisdictional Challenges and Cross-Border Operations

Jurisdictional issues constitute another major enforcement challenge. Many loan apps operate through **complex corporate structures** involving multiple entities across different jurisdictions. Data may be collected in India, processed on servers located abroad, and monetised through foreign affiliates. This fragmentation complicates the application of domestic laws and raises questions regarding jurisdiction, applicable law, and enforcement authority.

Cross-border data flows also strain institutional capacity. Mutual legal assistance treaties and international cooperation mechanisms are often slow and ill-suited to the rapid pace of digital transactions. In the absence of effective cross-border enforcement, operators can exploit jurisdictional loopholes to avoid accountability.

Additionally, the presence of informal or unregistered loan apps further exacerbates jurisdictional challenges. Such entities may disappear or re-emerge under different names, rendering enforcement actions reactive and ineffective.

### Regulatory Fragmentation and Overlapping Mandates

India’s regulatory response to data-driven economic offences is characterised by **institutional fragmentation**. Multiple authorities—including the Reserve Bank of India, data protection authorities, cybercrime cells, and consumer protection bodies—exercise partial jurisdiction over different aspects of digital lending.

While sector-specific oversight is necessary, the absence of a **coordinated enforcement framework** leads to gaps and overlaps. Regulatory bodies may focus narrowly on their mandates, overlooking systemic harms. For instance, data protection authorities may impose penalties for consent violations, while financial regulators address prudential concerns, leaving economic exploitation unaddressed as a criminal offence.

Fragmentation also burdens victims, who must navigate multiple forums to seek redress. This complexity discourages reporting and weakens deterrence. Without a unified approach, exploitative practices continue to fall through regulatory cracks.

### Resource Constraints and Capacity Deficits

Effective enforcement requires specialised technical expertise, yet regulatory and investigative agencies often lack adequate resources and trained personnel.

Understanding algorithmic models, data flows, and digital infrastructure demands interdisciplinary skills that are still developing within public institutions.

28.**National Crime Records Bureau (NCRB)**, *Crime in India* Reports (recent editions).
29.**Ministry of Home Affairs**, *Indian Cyber Crime Coordination Centre (I4C)* Scheme Documents.
30.**Comptroller and Auditor General of India (CAG)**, *Performance Audit on Cyber Crime Policing*
31.**Law Commission of India**, *Report No. 272* (2017).
32.**Supreme Court of India**, *Arnesh Kumar v. State of Bihar* (2014) 8 SCC 273.
33.**Parliamentary Standing Committee on Home Affairs**, *Report on Cyber Crime* (2022).
34.**Centre for Internet and Society (CIS)**, *State of Cyber Policing in India* (2020).

Capacity deficits lead to selective or delayed enforcement, enabling offenders to normalise exploitative practices. Over time, this erodes public trust in regulatory institutions and weakens the rule of law in digital markets.

### Proposing Legal and Policy Reforms to Address Exploitative Data Harvesting

In light of the identified challenges, this objective proposes a set of **legal and policy reforms** aimed at recognising, preventing, and prosecuting exploitative data harvesting as an economic crime. These reforms seek to move beyond fragmented compliance models towards a cohesive and deterrence-oriented framework.

### Enhancing Regulatory Coordination and Institutional Capacity

Addressing regulatory fragmentation requires the establishment of **inter-agency coordination mechanisms**. A centralised task force or nodal authority could facilitate information sharing, joint investigations, and coherent enforcement strategies.

Capacity building is equally critical. Regulators and law enforcement agencies must invest in technical expertise, forensic tools, and continuous training to keep pace with evolving technologies. Public-private collaboration, subject to safeguards, may also enhance enforcement effectiveness.

### Corporate and Algorithmic Accountability

Legal reforms should clarify standards of **corporate criminal liability** for data-driven offences. Companies must be held accountable for systemic failures, including negligent oversight of algorithms and third-party vendors.

Transparency and auditability requirements for algorithms used in lending and recovery processes should be mandated. Independent audits and explainability standards would enhance accountability and enable meaningful redress for affected individuals.

### Victim-Centric Remedies and Public Awareness

Finally, reforms must prioritise victim protection and access to remedies. Simplified grievance redress mechanisms, legal aid, and public awareness campaigns can empower borrowers to assert their rights. Recognising victims of data-driven exploitation within economic crime frameworks would ensure restitution and rehabilitation.

***35.j*****ustice B.N. Srikrishna Committee**, *Report of the Committee of Experts on a Data Protection Framework for India* (2018).

**36.Digital Personal Data Protection Act, 2023**, Sections 4–10, 27 and 33.

**37.NITI Aayog**, *Responsible AI for All* (2021).

**38.Parliamentary Standing Committee on Information Technology**, *Report on Citizens' Data Security and Privacy* (2021).

**39.National Human Rights Commission (NHRC), India**, *Advisory on Misuse of Digital Lending Apps* (2021).

**40.National Legal Services Authority (NALSA)**, *Legal Services to Victims of Cyber Crime* Schemes.

**41.Ministry of Home Affairs**, *Indian Cyber Crime Coordination Centre (I4C)* and **National Cyber Crime Reporting Portal**.

## BIBLIOGRAPHY

### BOOKS

- Shoshana Zuboff — *The Age of Surveillance Capitalism*
  A foundational analysis of how big tech monetises data and accumulates power. Wikipedia

- Dr. Rahul Matthan — *Data Protection Law in India*
  Practitioner's perspective on data protection (DPDP Act, compliance, enforcement). The Legal School
- Dr. Pavan Duggal — *Cyber Privacy in India*
  Focuses on cyber law and privacy, useful for understanding IT Act limitations and digital harms. The Legal School
- Dr. Apar Gupta — *Privacy Law: An Indian Perspective*
  Explores privacy rights and legal frameworks in India. The Legal School
- Udbhav Tiwari — *Data Privacy and Protection in India*
  Analyses India's data protection regime and legal gaps. IJLSSS

### JOURNAL ARTICLES

- Mahera Imam et al., *From Data to Discrimination: Gender, Privacy, and the Politics of Digital Surveillance*, **Synergy: Int'l Journal of Multidisciplinary Studies**
- **"Surveillance, privacy and the policy challenges: Decolonizing personal data protection in India,"***Journal of Digital Media & Policy* — critical policy analysis of India's data protection evolution. Intellect Discover
- Makanadar, *Digital Surveillance Capitalism and Cities: Data, Democracy and Activism*, **Humanities and Social Sciences Communications**

- *International Journal of Criminal, Common and Statutory Law*, Preksha Singh, *Dusk before the dawn? Critical analysis of the new data protection law* — critiques DPDP Act 2023 and enforcement gaps. Criminal Law Journal

- Md Jiyauddin, *Technical and Legal Aspects of Data Privacy in India: A Critical Analysis With Legal Provisions*, **IJLSSS** — detailed review of India's data privacy laws and technical compliance challenges. IJLSSS

- *Regulatory Approaches to Balancing Privacy Rights and Technological Innovation: A Comparative Analysis* — examines India DPDP alongside GDPR and CCPA frameworks. cdpp.co.in

## REFERENCE

1. Edwin H. Sutherland, *White Collar Crime*, Holt, Rinehart and Winston, 1949.
2. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, 2007.
3. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Praeger, 2010.
4. R.K. Sharma, *Cyber Laws in India*, AuthorPress, New Delhi, 2021. Indian legal framework, IT Act analysis, and recent cyber trends.
5. Aparna Vishwanathan Gupta, *Cyber Law: Indian and International Perspectives*, LexisNexis, 2015.Comparative approach (India–EU–US).
6. K. Arora & A. Bagri, *White Collar Crimes and Corporate Frauds in India*, Universal Law Publishing, 2019.

B. CYBERCRIME, TECHNOLOGY & AI (ADVANCED SOURCES)

7. Kim-Kwang Raymond Choo, “The Cyber Threat Landscape: Challenges and Future Research Directions”, *(2011) 30 Computers & Security 719.*
8. Mariarosaria Taddeo & Luciano Floridi, “How AI Can Be a Force for Good”, *(2018) Science 751*.
9. Nguyen T.T. et al., “Deep Learning for Deepfakes Creation and Detection”, *(2019)*.
10. Monica T. Whitty, “Anatomy of the Online Dating Scam”, *(2015) 28(4) Security Journal 443.*