PROTECTING DIGITAL INTEGRITY: INDIA'S CYBERSECURITY LAW REVOLUTION

Sai Sibani Panda, School of Law, KIIT Deemed to be University, Patia, Bhubaneswar, Odisha, India[1]

ABSTRACT

The increasing digitisation of India, exemplified by the Aadhaar initiative, has significantly enhanced service delivery; however, it has also revealed critical vulnerabilities in data security. Cybersecurity jurisprudence in India is evolving rapidly, shaped by statutes like the Information Technology Act, 2000, and landmark judgments such as Justice K.S. Puttaswamy v Union of India. Judicial pronouncements have increasingly recognised the fundamental right to privacy and emphasised the need for stronger data protection standards. However, enforcement mechanisms and comprehensive cybersecurity-specific legislation are still developing to meet the challenges of a digitised economy. This research paper examines the evolution of cybersecurity in India, particularly following the Aadhaar breach, which represents a pivotal moment in this context. The author employs a doctrinal research methodology to analyse primary sources such as legislation and policies, as well as secondary sources including news articles and research studies, to effectively address the key research questions. A comparative analysis is also conducted against global best practices, such as the EU's GDPR. The discussion highlights India's progress in establishing regulatory frameworks, however, major challenges persist. India's breach notification timeline of six hours is impractically stringent; the regulatory framework remains narrowly focused on digital data alone; the Data Protection Board is not yet fully operational; and public transparency about breaches is weak. Furthermore, protections for ethical cybersecurity research are ambiguous, unlike international standards that encourage responsible disclosures. The findings reveal that while India's regulatory landscape has improved significantly since the Aadhaar breach, critical gaps in enforcement, scope continue to hamper full alignment with global norms. The author concludes that to make India a global leader in data privacy and cybersecurity, it is essential to implement stronger measures, provide broader protections, and engage the public.

Keywords: Data Protection, Aadhaar Breach, Cybersecurity, Cyberspace, Encryption

[1] Student, School of Law, KIIT Deemed to be University, Patia, Bhubaneswar, Odisha, India

I. INTRODUCTION

The rapid digitisation of India has fundamentally transformed the way personal data is collected, stored, and utilised. The Aadhaar project, initiated in 2009 by the Unique Identification Authority of India (UIDAI), aimed to provide a unique 12-digit identification number to residents based on their biometric and demographic data. While Aadhaar promised to revolutionize public service delivery and reduce identity fraud, it also headed to new vulnerabilities concerning data protection and cybersecurity.

In 2018, the Aadhaar ecosystem witnessed one of its most serious crises: an investigative report revealed that access to the entire Aadhaar database could be obtained for a mere sum of INR 500 by unauthorised individuals[2]. This breach revealed major weaknesses in the system's security and raised serious questions about whether India's laws and regulations protect data effectively. The incident not only showed problems in operations but also highlighted a bigger issue: there is no complete cybersecurity policy or data protection system to safeguard the digital identities of over a billion people.

The Aadhaar data breach acted as a catalyst, intensifying public discourse around privacy, leading to landmark judicial interventions like the Supreme Court's recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*[3]. Subsequently, policy initiatives such as the Personal Data Protection Bill, 2019, and later the Digital Personal Data Protection Act, 2023, sought to address these gaps.

This research paper explores how cybersecurity is changing in India, especially after the Aadhaar breach, which marked an important turning point. It examines the laws, policy changes, and court decisions that are shaping India's data protection rules. By reviewing existing literature and analysing legal discussions, the paper aims to assess whether India’s efforts have effectively addressed the risks that the Aadhaar incident revealed.

II. LITERATURE REVIEW

This peer-reviewed paper[4] examines Aadhaar’s biometric and demographic data vulnerabilities, highlighting systemic weaknesses in encryption, authentication, and third-party

[2] Rachna Khaira, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details' *The Tribune* (Chandigarh, 4 January 2018),Rs 500, 10 minutes, and you have access to billion Aadhaar details - The Tribune.
[3] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1
[4] Debanjan Sadhya and Tanya Sahu, 'A critical survey of the security and privacy aspects of the Aadhaar framework' (2024) 140 Computers & Security ,https://doi.org/10.1016/j.cose.2024.103782.

integrations. Additionally, the paper highlights the need for updated studies, as the Aadhaar framework is constantly evolving with new policies and regulations. It also emphasizes the lack of detailed analysis on linkage attacks, which occur when databases linked to Aadhaar-enabled schemes are compromised.

The literature on cyberattacks in India highlights alarming trends in recent years[5]. Studies have emphasised the vulnerabilities in government platforms, healthcare systems, and critical sectors like energy. Notable incidents include the AIIMS cyberattack, RailYatri data breach, and the exploitation of the UP-Marriage Assistance Scheme. Researchers advocate robust security measures, employee training, and transparency as essential strategies for mitigating risks. The literature underscores the importance of proactive threat detection, encryption, and incident response plans to fortify digital infrastructure and safeguard sensitive information.

The literature on Aadhaar's security highlights its vulnerabilities despite robust biometric measures[6]. Studies reveal frequent data breaches in departments like passport and land registration offices, compromising sensitive information. Researchers propose systems like UBSAFE to mitigate threats, emphasizing encryption, multi-factor authentication, and regular audits. The literature underscores the need for stringent cybersecurity policies and public awareness to safeguard identity and financial assets.

The Aadhaar system, while transformative in governance, faces critical challenges in privacy and security. Research highlights[7] risks like unauthorized access, data breaches, and linkage attacks. The Puttaswamy judgment underscored privacy as a fundamental right, advocating stronger legal frameworks. Comparative studies with systems like the EU's GDPR emphasize decentralized security and privacy-by-design principles. Critics also point to Aadhaar's role in marginalizing vulnerable populations, despite its efficiency in welfare distribution. Addressing these issues requires proactive policymaking and continuous evaluation of societal impacts.

The news article[8] highlights a significant data breach involving Aadhaar and passport information of 815 million Indians, which was reportedly put up for sale on the dark web. The

[5] Sattrix InfoSec, 'Top 25 Biggest Cyber Attacks in India: Major Data Breaches & Cybercrime' (2024) https://www.sattrix.com/blog/biggest-cyber-attacks-in-india.

[6] Reshmi Maulik, 'A Review on Mitigating Security Threats in Aadhaar' (2024) 15 INDJCSE https://doi.org/10.21817/indjcse/2024/v15i3/241503027.

[7] Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma, 'Privacy and Security of Aadhaar: A Computer Science Perspective' (2023) https://www.cse.iitd.ac.in/~suban/reports/aadhaar.pdf.

[8] Ashutosh Mishra, 'Aadhaar data of 815 million on sale on the dark web, says report' (Business Standard, 30 October 2023) https://www.business-standard.com/india-news/aadhaar-data-of-millions-of-indians-put-on-sale-on-the-dark-web-reports-123103000993_1.html.

breach raises serious concerns about the security measures of the Unique Identification Authority of India (UIDAI) and the vulnerability of biometric data storage. Experts emphasize the need for robust cybersecurity strategies, including encryption, multifactor authentication, and regular audits, to prevent such incidents. The article also discusses the broader implications of digital identity theft, including financial fraud and misuse of personal information, underscoring the urgency for stronger data protection frameworks

The news article[9] discusses a significant data breach involving the personal information of approximately 815 million Indians, including Aadhaar and passport details, which was discovered on the dark web. The breach, attributed to a threat actor named 'pwn0001,' has raised serious concerns about India's digital infrastructure and data security measures. The compromised data is suspected to have originated from the Indian Council of Medical Research (ICMR) database. This incident highlights vulnerabilities in India's digital public infrastructure, which relies heavily on Aadhaar for governance and service delivery. It underscores the urgent need for robust cybersecurity frameworks and proactive measures to safeguard sensitive information.

The Aadhaar system, while transformative in governance and service delivery, has faced significant scrutiny over privacy and security concerns. Reports highlight[10] vulnerabilities such as unauthorized access, data breaches, and misuse of biometric data. The World Economic Forum's Global Risks Report identified Aadhaar as the largest data breach globally, with sensitive information of over 1.1 billion individuals exposed. Critics argue that centralized data storage and insufficient safeguards make the system susceptible to cyberattacks. Despite its efficiency in welfare distribution, Aadhaar's challenges underscore the need for decentralized security measures, robust legal frameworks, and privacy-by-design principles to protect citizens' data and rights.

The article on India's Digital Personal Data Protection (DPDP) Act, 2023[11] outlines key rules for reporting data breaches. It stresses the importance of being transparent and accountable, defining a breach as unauthorized actions that affect data security. Organizations, called

[9] Editorji News Desk, 'Major data breach exposes 815 million Indians' personal information on dark web' (Editorji, 31 October 2023) https://www.editorji.com/business-news/major-data-breach-exposes-815-million-indians-personal-information-on-dark-web-1698722903431

[10] Yogesh Sapkale, 'Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast' (Moneylife, 19 February 2019) https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html.

[11] Advocate (Dr.) Prashant Mali, 'Data breach reporting requirements in India' (November 1, 2024) https://dpdpa.com/blogs/databreachreporting.html.

fiduciaries, must quickly notify the Data Protection Board and affected individuals about the breach, detailing what happened and how they will address it. The article suggests preventive measures like forming response teams and conducting security audits. It also highlights examples of breaches at MobiKwik, Air India, and Aadhaar, while noting gaps like unclear reporting timelines.

III. RESEARCH GAP

The research gap identified through various literature reviews pertains to the insufficient evaluation of India's legal and institutional responses to data breaches, particularly concerning Aadhaar. While extensive literature highlights technical vulnerabilities and ethical issues related to Aadhaar, there is a lack of comprehensive analysis on the effectiveness of recent legislative measures, such as the Digital Personal Data Protection Act, 2023. This gap hinders our understanding of how well these laws address the specific challenges posed by data breaches and their implications for data privacy and security. Addressing this gap is essential for assessing the strength of India's data protection framework.

IV. RESEARCH QUESTIONS

1. How have India's legislative and policy frameworks evolved in response to the Aadhaar data breach and similar cybersecurity incidents?
2. How do Indian regulatory and enforcement responses to data breaches compare to global best practices?

V. METHODOLOGY

The author has adopted a doctrinal research methodology to analyse primary sources such as legislation and policies, as well as secondary sources including news articles and research studies, to effectively address the key research questions.

VI. INDIA'S LEGISLATIVE AND SECURITY POLICY FRAMEWORK IN RESPONSE TO DATA BREACH: AN OVERVIEW

A. DISCUSSION

India has launched large digitization projects like Aadhaar. However, it faced important questions about its laws and policies after several major cybersecurity incidents. In 2018, a breach of Aadhaar data exposed sensitive information of millions of people. This event sparked a debate both in India and internationally about data privacy, security, and whether India's legal

frameworks are strong enough.

The author will analyze how India's laws, policies, and court decisions have changed in response to Aadhaar-related breaches and cybersecurity issues. This will address the first research question.

Aadhaar Data Breach: The Catalyst for Reform

A 2018 report by "The Tribune" exposed a serious problem in the Aadhaar system. It revealed that unauthorised people could access sensitive Aadhaar data for as little as ₹500[12]. This worrying discovery highlighted multiple weaknesses in the system that put citizens' data at risk.

Further investigations showed that the system had several flaws, including weak encryption and vulnerabilities linked to third-party vendors who manage and store biometric and personal information. These issues raised major concerns about the safety and trustworthiness of the data belonging to millions of Indian citizens.

This incident served as a crucial warning, showing that current laws and regulations were not enough to protect personal data on such a large scale. In response to these findings, there was an urgent need for major changes in laws and policies across various sectors. This urgency led to a review of existing data protection laws and prompted stakeholders to adopt stricter security measures and improve transparency in how they handle data. The push for reform stressed the importance of protecting individual privacy rights and building a stronger digital system to avoid similar data breaches in the future.

Legislative Frameworks Before and After the Aadhaar Breach

The provisions related to data governance prior to the Aadhar breach have been discussed by the author and is substantiated as follows:

The Information Technology Act, 2000 (IT Act); it serves as India's foundational legislation concerning cyber issues. Although it was not initially crafted with personal data protection in mind, significant amendments introduced provisions relevant to cybersecurity. Firstly, Section

[12] Ritu Sarin, "Rs 500, 10 minutes, and you have access to billion Aadhaar details" *The Tribune* (4 January 2018) https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361 accessed .

43A was added, imposing liability on corporate bodies that fail to safeguard sensitive personal data. Secondly, Section 72A was incorporated, which penalizes the unauthorized disclosure of personal information. Lastly, an adjudicatory mechanism was established for the resolution of disputes through adjudicating officers and the Cyber Appellate Tribunal.

However, the protections in the IT Act were too broad and reactive. They did not have the foresight needed to handle the complex issues of managing biometric data. This became clear after the Aadhaar breach, which exposed major weaknesses and showed that the safeguards for sensitive personal information were not enough[13].

Judicial intervention;In the case of *Justice K.S. Puttaswamy v Union of India (2017)*, the Supreme Court of India made a unanimous decision that recognised the right to privacy as a fundamental part of the right to life and personal liberty under Article 21 of the Constitution. This key ruling confirmed the legal status of the Aadhaar scheme but criticised the weak data protection measures linked to it.

Following this decision, the government set up the B.N. Srikrishna Committee in August 2017, appointing experts to tackle the urgent issue of data protection in India. Led by Justice B.N. Srikrishna, the committee researched and discussed the topic extensively, finishing their report in July 2018. This report included a draft Data Protection Bill and suggested many ways to strengthen privacy laws in the country.

The main suggestions included strict limits on collecting and processing personal data, creating a Data Protection Authority to ensure compliance, introducing the right to be forgotten, and requiring data localisation. Together, these actions aim to build a strong system that protects individuals' privacy rights in India's rapidly changing digital environment.

Digital Personal Data Protection Act 2023; Subsequently, responding directly to the vacuum exposed by Aadhaar-related issues and the *Puttaswamy* judgment, Parliament enacted the Digital Personal Data Protection Act, 2023[14]. It is India's first comprehensive legislation dedicated exclusively to protecting personal data, a major milestone prompted, in part, by incidents like the Aadhaar breach. The government’s recent introduction of the Digital Personal

[13] Apar Gupta, "The Aadhaar Judgment and the Future of Data Protection Law in India" (2018) 3 *Indian Law Review* 79.
[14] Digital Personal Data Protection Act 2023 (India).

Data Protection (DPDP) Act signifies a major step toward strengthening data security. One key aspect of the DPDP Act is its emphasis on data breach reporting, a critical measure to ensure transparency, accountability, and prompt response in the event of a security incident. With millions of people using online services and transacting digitally, data breaches in India are no longer hypothetical concerns; they are real threats that affect individuals and organisations daily.

Data breach reporting requirements serve multiple purposes. For individuals, prompt notification provides an opportunity to take protective measures, such as changing passwords or monitoring financial accounts. For regulatory bodies, breach reporting enables oversight and intervention, where necessary, to protect public interests. For businesses, compliance with breach reporting regulations enhances transparency and helps build trust with customers and stakeholders.

Under the DPDP Act, if there is a personal data breach, a Data Fiduciary must inform each affected Data Principal and the Data Protection Board. The Draft Rules explain how these notifications should be made, including when and what details need to be included. A personal data breach is defined as any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data. This can compromise the confidentiality, integrity, or availability of the data. Data Fiduciaries must report all types of personal data breaches, regardless of severity or impact on the Data Principal. The Act does not set any materiality thresholds or specific timelines for reporting.

"Section 4" details the responsibilities of Data Fiduciaries, which include ensuring data accuracy and completeness, implementing reasonable security measures to prevent breaches, and deleting personal data once it is no longer needed. "**Section 6"** outlines the requirements for valid consent, which must be free, specific, informed, unconditional, and clear. Data Principals also have the right to withdraw consent anytime, and this should be as easy as giving consent.

"Section 18" establishes the Data Protection Board of India, which oversees compliance, imposes penalties, and resolves disputes. "**Section 24"** specifies penalties for not following the Act, including for security breaches and failing to notify about data breaches.

The Indian Computer Emergency Response Team (CERT-In). The DPDP Act is not the

sole regulation imposing a reporting requirement for data breaches. The existing cybersecurity framework also mandates reporting of cybersecurity incidents, which may include personal data breaches, to the Cert-In. In the absence of any conflicting information, both sets of regulations will be applicable. It is the national nodal agency for responding to computer security incidents as and when they occur.

It was established under Section 70B of the Information Technology Act, 2000. The Government of India has established and authorised the Cert-In to collect, analyse and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities.

Prior to the 2022 amendment, it operated mainly by issuing advisories and best practice guidelines and requesting, but not mandating, the reporting of cybersecurity incidents. Subsequently 2022, the Indian Computer Emergency Response Team (CERT-In) issued updated guidelines requiring[15]

Firstly, **Mandatory Incident Reporting within 6 Hours**

- Any cybersecurity incident must be reported to CERT-In within six hours of becoming aware of it.This includes incidents like data breaches, ransomware attacks, server hacks, DDoS attacks, etc.

Secondly, **Mandatory Log Retention**

- Entities must maintain logs of all ICT (Information and Communication Technology) systems for at least 180 days. These logs must be stored within India.

Thirdly, **Mandatory Time Synchronisation**

- All ICT systems must synchronise their clocks to the National Informatics Centre's Network Time Protocol (NTP) server or other government-approved time sources. This ensures consistency in forensic investigations.

These measures aim at early detection and response, crucial in minimising breaches like those

[15] CERT-In, 'Directions Under Section 70B of the IT Act, 2000' (28 April 2022).

involving Aadhaar.

These incidents can be reported to Cert-In via (i) email (incident@cert-in.org.in), (ii) phone (1800-11-4949), or (iii) fax (1800-11-6969). The reporting methods and formats are available at www.cert-in.org.in and will be updated from time to time. The compliance obligations under the Cyber Security Directions extend to all entities that have computer systems, networks and/or resources in India, irrespective of whether the entity is incorporated in or outside India.

B. KEY FINDINGS

The Aadhaar data breach served as a significant inflexion point, exposing critical vulnerabilities in India's digital governance structures and catalysing substantial legal and policy reforms. A primary finding is that India's pre-existing legislative frameworks were woefully inadequate to handle cybersecurity threats involving large-scale biometric data. The Information Technology Act, 2000, while pioneering for its time, was primarily designed to facilitate electronic commerce and punish cybercrimes such as hacking or identity theft, rather than to offer robust protections for personal data. The Act's limited provisions, particularly Sections 43A and 72A, lacked detailed procedural safeguards, comprehensive breach notification mandates, or sector-specific security standards for critical databases like Aadhaar. This gap created a regulatory vacuum that the Aadhaar Act, 2016 failed to fill, as it focused more on the operational aspects of the Unique Identification Authority of India (UIDAI) and less on data protection protocols or redressal mechanisms for breaches.

The second major finding is that judicial intervention played a pivotal role in steering India toward a rights-based framework for data protection. The landmark Justice K.S. Puttaswamy (Retd) v Union of India (2017) judgment recognized privacy as a fundamental right under Article 21 of the Constitution, fundamentally shifting the legal terrain. By placing the right to privacy on par with other fundamental rights, the Supreme Court compelled the legislature to prioritize citizen privacy in all future digital initiatives. Furthermore, in the subsequent Puttaswamy judgment (2018), the Court imposed specific restrictions on the Aadhaar framework, especially prohibiting private sector use of Aadhaar authentication services, thereby directly addressing some of the vulnerabilities that enabled previous breaches. These judicial decisions created a constitutional imperative that could not be ignored, forcing both legislative and executive arms to rethink cybersecurity and personal data protection comprehensively.

A third critical finding is that the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) represents a watershed moment in India's legal landscape. The DPDPA fills a longstanding void by articulating a comprehensive set of rights for data principals (individuals) and obligations for data fiduciaries (entities that process data). It institutionalises principles such as consent-based data processing, purpose limitation, data minimisation, and grievance redressal. Particularly important is the creation of a robust penalty regime with fines scaling up to ₹250 crore for breaches, thereby significantly raising the cost of non-compliance. Unlike the piecemeal protections under the IT Act, the DPDPA introduces systemic obligations such as mandatory data breach reporting and the appointment of data protection officers, indicating a move toward a proactive and preventive model of cybersecurity governance. However, some critics argue that the Act grants wide exemptions to government agencies, which could undercut its overall effectiveness.

Fourth, administrative measures such as CERT-In's updated 2022 guidelines reflect a maturing approach toward cybersecurity incident management. The mandatory six-hour reporting window for cyber incidents and the emphasis on time-synchronised logging are practical steps to ensure early detection and rapid response to breaches. These measures, while operational in nature, signify a shift from reactive to preventive cybersecurity strategies.

Fifth, the gap between law and enforcement remains a significant challenge. Despite progressive legislation and policies, India's institutional capacity to enforce data protection norms is still underdeveloped. The newly created Data Protection Board under the DPDPA is yet to become fully operational. Past experiences with bodies like the Cyber Appellate Tribunal, which became defunct due to a lack of appointments, underscore the risks of creating institutions without ensuring their sustained functionality. Furthermore, there is a lack of widespread public awareness regarding data rights and grievance mechanisms, which limits the potential impact of new laws at the ground level.

Finally, the balancing act between privacy and national security continues to evolve. India’s emerging data protection regime tries to strike a delicate balance between empowering citizens and equipping the state with tools to protect national interests. While laws now better safeguard privacy, broad government exemptions under the DPDPA and expansive surveillance powers under other laws, such as the Telegraph Act and IT Act, suggest that the equilibrium between privacy rights and state security is still heavily tilted toward the government.

In conclusion, the Aadhaar data breach and subsequent incidents exposed systemic flaws but also accelerated a vital legal transformation. India's cybersecurity and data protection landscape today is significantly more advanced, rights-conscious, and structured than it was a decade ago. Nonetheless, full realization of privacy rights and cybersecurity resilience will depend not only on the laws themselves but also on consistent enforcement, institutional integrity, judicial vigilance, and a citizenry that actively demands accountability.

VII. COMPARISON OF INDIAN REGULATORY AND ENFORCEMENT RESPONSES TO DATA BREACHES WITH GLOBAL BEST PRACTICES

A. DISCUSSION

The global increase in cyber threats has forced countries to create robust data protection and breach response frameworks. India, with its expanding digital economy, has recognised the need for stringent data protection laws. However, a detailed comparison between India's regulatory responses and global best practices, notably the EU's General Data Protection Regulation (GDPR), reveals significant differences, strengths, and gaps. The comparison will be substantiated in the following points.

Firstly, on the aspect of the regulatory framework, India's primary legislative framework addressing data protection is the Digital Personal Data Protection Act, 2023 (DPDPA). The Act seeks to protect digital personal data, setting obligations for "Data Fiduciaries" and establishing the "Data Protection Board of India" for enforcement. The Indian Computer Emergency Response Team (CERT-In) complements this framework by mandating cybersecurity incident reporting within six hours[16].

In contrast, the GDPR regulates all personal data processing activities, both online and offline, across the European Union. It enshrines fundamental rights to privacy and imposes breach notification within 72 hours[17].

Secondly, jurisdictional scope: The DPDPA focuses only on digital personal data, omitting

[16] Indian Computer Emergency Response Team (CERT-In) 'Directions relating to information security practices' (28 April 2022) https://www.cert-in.org.in

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

physical records[18]. This digital-only scope limits India's protection compared to the GDPR, which applies universally to all forms of personal data. Furthermore, GDPR explicitly extends its jurisdiction extraterritorially, applying to any entity processing EU citizens' data, regardless of location[19]. While India's DPDPA can apply to global entities processing Indian citizens' data, its extraterritorial enforcement mechanisms remain weak due to the absence of detailed cross-border cooperation provisions, unlike GDPR's robust framework.

Thirdly, the breach notification requirements: India mandates breach reporting to CERT-In within six hours of identification[5]. This is significantly stricter than GDPR's 72-hour notification rule. While a shorter window ensures faster response, it may result in rushed or incomplete reporting. In practice, companies often struggle to fully understand and assess a breach within six hours, raising concerns over feasibility and quality of information shared.

Fourthly, the enforcement mechanism: India's DPDPA proposes setting up the Data Protection Board of India (DPBI) to adjudicate breaches and impose penalties[7]. The maximum fine under the DPDPA can reach ₹250 crores (approx. USD 30 million), depending on the gravity of the offence. [8]

Comparatively, GDPR empowers Data Protection Authorities (DPAs) to impose fines up to €20 million or 4% of annual global turnover, whichever is higher.[9] Furthermore, GDPR enables private enforcement by individuals seeking damages, strengthening accountability.

India's regime is largely top-down, with limited scope for individual compensation claims unless the government enacts additional procedural laws to operationalise it.

Furthermore, on the aspect of public awareness and accountability: One key difference is the level of public engagement and rights awareness. The GDPR mandates that controllers maintain transparency with individuals about breaches that pose high risks[20]

While DPDPA grants rights like grievance redressal and data portability, it lacks detailed mechanisms ensuring public notification after serious breaches, unless directed by the Data

[18] Digital Personal Data Protection Act 2023 (India), s 2.
[19] GDPR (n 2) art 3.
[20] GDPR (n 2) art 34.

Protection Board[21]. In the absence of proactive notification duties, users might remain unaware of compromised data unless the regulator intervenes.

Lastly on Protection of Research and Ethical Hacking: Under the GDPR, ethical hackers and researchers are protected when acting within the law and contributing to public security. India's earlier drafts criminalised unauthorised re-identification of anonymised data, even for research purposes, which drew criticism for chilling legitimate cybersecurity efforts[22].

The final version of DPDPA relaxes some restrictions but still leaves ambiguity around lawful research exceptions. This contrasts with global best practices that emphasize the promotion of ethical research to enhance cybersecurity.

B. KEY FINDINGS

While India has made notable progress with the introduction of the Digital Personal Data Protection Act, 2023 (DPDPA) and enhanced CERT-In guidelines, significant challenges remain in its regulatory and enforcement framework for data breaches. A major challenge lies in the six-hour breach notification requirement, one of the strictest globally. Although intended to ensure rapid response, this timeframe is often unrealistic, risking rushed, inaccurate reports and creating a burden for organizations that may not have completed a full breach assessment within that period. Another critical shortcoming is the limited scope of the DPDPA, which protects only digital personal data, unlike the GDPR, which safeguards all personal data regardless of format. This leaves important non-digital records without comprehensive protection in India.

Enforcement also faces hurdles. The Data Protection Board of India (DPBI), responsible for investigating breaches and imposing penalties, remains non-operational as of 2025, creating a regulatory vacuum that undermines the credibility of the law. Although the DPDPA allows for substantial fines, there is currently no clear mechanism for individuals to seek direct compensation, contrasting sharply with the individual redress rights under the GDPR.

Another pressing challenge is India's **inadequate protection for ethical cybersecurity research**; despite some relaxations, the law still leaves grey areas that could discourage

[21] Digital Personal Data Protection Act 2023 (India), s 14.
[22] WIRED, 'India’s Data Protection Bill Threatens Global Cybersecurity' (WIRED, 19 August 2022) https://www.wired.com/story/opinion-indias-data-protection-bill-threatens-global-cybersecurity/

researchers from identifying vulnerabilities, a vital component of a healthy cybersecurity ecosystem.

In addition, India's lack of a clear public notification requirement following major breaches means that affected individuals might not be informed unless regulators intervene, weakening transparency and accountability compared to the mandatory disclosure obligations under GDPR.

To sum up, India's regulatory framework marks an important advancement; however, it still confronts major obstacles: unfeasible compliance deadlines, limited scope of data protection, operational lags, inadequate rights for individuals, ambiguous research safeguards, and a lack of transparency. It will be crucial to tackle these challenges promptly for India to align with global benchmarks and truly enhance its data protection and breach response abilities.

VIII. CONCLUSION

The Aadhaar data breach marked a watershed moment in India's journey toward stronger cybersecurity and data protection frameworks. It exposed significant flaws in existing legislative structures, notably the Information Technology Act, 2000, which was not designed to address the complexities of biometric and personal data management. In response, India undertook major legal reforms, with judicial interventions such as the Puttaswamy judgment recognising privacy as a fundamental right and legislative developments culminating in the Digital Personal Data Protection Act, 2023 (DPDPA).

Despite these advancements, critical challenges persist. The DPDPA’s exclusive focus on digital data leaves non-digital information vulnerable, and the extremely stringent six-hour breach notification timeline may hinder rather than help effective compliance. Moreover, although the DPDPA sets up the Data Protection Board of India to ensure accountability, delays in its operationalization weaken enforcement potential. India's regulatory approach also falls short in ensuring transparency toward data principals, especially concerning breach notifications, which are largely regulator-dependent rather than proactively mandated.

Comparative analysis with global standards like the GDPR highlights that while India has incorporated key principles such as consent-based processing, purpose limitation, and penalty mechanisms, gaps remain in areas like cross-border enforcement, individual compensation

rights, and clear safeguards for ethical cybersecurity research. Additionally, public awareness around data rights and the importance of cybersecurity remains low, potentially limiting the effectiveness of legislative measures.

Thus, while India's legal landscape has significantly evolved post-Aadhaar, bridging the gap between legislative intent and effective implementation is crucial. Strengthening institutional capacity, enhancing public engagement, safeguarding researchers, and ensuring prompt and meaningful breach disclosures will be vital to achieving a truly resilient and rights-based cybersecurity environment.