2026 Volume: 02 Issue: 07 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-14

FROM CONSENT TO CONTROL: RETHINKING DATA PRIVACY LAWS AMIDST RISING AI AND CYBER FRAUD THREATS

[*1]Pankaj Kumar and [2]Amritansh Verma

[1]Assistant Librarian Babu Banarasi Das University, Lucknow (U.P.) India-226028.

[2]BBA LL.B. Babu Banarasi Das University, Lucknow

Article Received: 17 June 2026
Article Revised: 07 July 2026
Published on: 27 July 2026

***Corresponding Author: Pankaj Kumar**
Assistant Librarian Babu Banarasi Das University, Lucknow (U.P.) India-226028.

DOI: https://doi-doi.org/101555/ijrpa.8359

ABSTRACT

The integration of Artificial Intelligence (AI) into data-driven systems has significantly challenged existing legal and ethical frameworks, particularly concerning data privacy and regulatory oversight. This paper critically examines how AI's dependence on massive data collection and algorithmic processing poses threats such as unauthorized surveillance, biometric data misuse, and lack of transparency in decision-making. Through real-world examples, the study highlights how AI technologies can both support and undermine privacy rights.

It further explores the adequacy of current legal instruments like the GDPR in addressing these concerns, noting critical gaps in consent, accountability, and explainability. The dual role of AI in enhancing cybersecurity and creating new vulnerabilities is also discussed. Ultimately, the paper calls for adaptive legal reforms that balance innovation with robust data protection and uphold individual rights in the digital age.

KEYWORDS: Artificial Intelligence (AI), Data Privacy, Cybersecurity, Cyber Fraud, Data Protection Laws, GDPR, Biometric Data, Algorithmic Bias, Legal Frameworks, and Consent Mechanism.

1. INTRODUCTION

In early 2024, global regulatory bodies are increasingly focusing on artificial intelligence (AI), with the European Union nearing finalization of its AI Act, and countries like the UK, China, and the US also pushing regulatory initiatives. In the US, although there is no federal

law specifically governing AI yet, federal and state agencies are working to interpret and expand existing laws to address AI concerns.

A major area of concern is the intersection of AI and data privacy. Since AI systems, particularly generative AI like ChatGPT, rely heavily on vast amounts of data, including personal information, their development directly affects privacy rights. Current privacy laws, often based on older frameworks like Fair Information Practices, are seen as inadequate to tackle the broad societal risks posed by AI. These include not just individual harms but large-scale implications for data control and consent. [1]

The paper emphasizes that while privacy laws exist, they do not sufficiently regulate the data pipelines that feed AI systems. As AI continues to grow, the demand for personal data will also increase, risking further erosion of privacy. The authors call for an urgent rethinking of privacy regulations, suggesting that current frameworks must evolve to address both individual and societal privacy challenges in the age of AI.

2. Current Landscape of Data Privacy Laws

2.1 Digital Personal Data Protection (DPDP) Act 2023 [2]

The Digital Personal Data Protection (DPDP) Act 2023 is a key piece of legislation aiming at protecting individuals' personal data in India. It defines the responsibilities of data fiduciaries, offers a framework for data rights, and imposes sanctions for noncompliance. Below is a full analysis of the essential sections, as well as simulated footnotes for context.

(i) Personal Data Protection

According to the Act, sensitive personal data, such as financial or health information, needs to be better protected. Personal data is defined as identifiable information; such as names or contact details. Additionally, the government can designate some data as essential personal information, which might be subject to more stringent regulations, such as requiring storage inside India.

(ii) Data Principal and Data Fiduciary

The person whose personal information is being processed and who has privacy rights is known as a data principal. Any business or government that gathers or handles this data is considered a data fiduciary and is required to do so in a responsible, open, and transparent manner while adhering to stringent data protection regulations.

(iii) Rights of Individuals (Data Principals) [2]

The DPDP Act gives Data Principals a number of rights to manage and safeguard their personal information:

Right to Information: Data Principals have the right to know how their data is being processed, including its recipients, purpose, and length of retention.
Right of Access: People are entitled to see the personal information that a data fiduciary has on them.
Right to Correction: People have the ability to ask for data that is out-of-date or erroneous to be corrected.
Right to Erasure: If the data processing was illegal or no longer required for the reasons for which it was gathered, data principals have the right to request that their data be deleted.
Consent and Withdrawal Rights: Free, informed, explicit, and unequivocal consent is required. Unless mandated by law, data principals have the right to revoke their permission at any moment, in which case processing must stop. [4]
The right to redress grievances: A Data Principal may file a complaint with the Data Fiduciary about how their data is handled. They may take the issue to the Indian Data Protection Board if they are not pleased.
Right to Nominate: In the event of death or disability, a data principal may designate another person to execute their rights.
The right to be informed: Data fiduciaries are required to give explicit notice of the data being gathered, its intended use, storage, and sharing. [5]

The right to data portability enables people to move their data across data fiduciaries, usually when they switch providers or services.

Here's a **table chart** comparing the **GDPR**, **CCPA**, and **DPDP Act 2023 (India)** based on their **strengths and weaknesses**:

Feature	GDPR (EU)	CCPA (California)	DPDP Act 2023 (India)
Scope	All personal data; global applicability	Applies to California residents; focused on data sales	Covers digital personal data; includes extraterritorial scope [6]
Individual Rights	Broad: access, erasure, data portability	Right to know, delete, and opt-out of data sale	Similar to GDPR + nomination rights and data portability
Consent Requirements	Explicit and specific consent required	Implied consent in some cases	Explicit consent required; withdrawal permitted
Data Localization	Not required	Not required	Required for sensitive data; more categories may be added
Enforcement Body	Independent DPAs; fines up to 4% of global turnover	California Attorney General; fines are capped	Government-appointed Data Protection Board; high penalties

Cross-border Transfers	Restricted; must meet Schrems II standards	No specific legal restrictions	Permitted, except to countries restricted by the Indian government
SME Impact	High compliance cost and complexity	Moderate impact	To be determined upon full implementation

Sources: The comparative analysis on data protection frameworks draws from a wide range of industry reports, legal insights, and technology blogs. Key insights regarding regulatory complexity, cost burdens on SMEs, data localization mandates, and enforcement mechanisms have been drawn from sources such as ETCISO.in, Airacle Labs, Borneo.io, CookieHub, The Sun, DigiLaw India, Lawctopus, NovoJuris, arXiv, Wikipedia, Reuters, and NoAndT.

2.2 Case Studies: Breaches & Implications in Data Protection

2.2.1 Meta Platforms (Facebook) – EU–US Data Transfers

Meta was fined €1.2 billion by Ireland, the company's principal EU privacy authority, in 2023 for moving EU user data to the United States via non-compliant procedures under the General Data Protection Regulation (GDPR). This enforcement followed the Schrems II decision, which invalidated the Privacy Shield agreement and questioned the adequacy of transatlantic data protection systems. The case highlighted legal ambiguities surrounding EU-US data transfers, as well as the limits of relying only on Standard Contractual Clauses (SCCs) to assure an identical degree of data protection. [7]

2.2.2 Google – CNIL Fine, 2019

The French data protection body, Commission Nationale de l'Informatique et des Liberties (CNIL), penalized Google €50 million for violating the GDPR due to a lack of transparency, inadequate user permission for tailored advertising, and opaque data processing procedures. This important ruling emphasized the GDPR's role in regulating algorithmic profiling and protecting user rights by challenging non-consensual behavioural advertising techniques used by digital behemoths. [8]

2.2.3 WhatsApp Ireland – €225 Million Fine, 2021

The Irish Data Protection Commission (DPC) fined WhatsApp €225 million for failing to fully tell users about how their personal data was shared with its parent firm, Meta Platforms, therefore violating the GDPR's transparency rules. This hefty penalty emphasized the crucial need of clear user communication, strong permission channels, and complete transparency in inter-company data sharing policies, laying the groundwork for enhanced responsibility in data governance. [9]

2.2.4 India: Hypothetical Learning from DPDP, 2023

The Digital Personal Data Protection Act, 2023, was adopted in India, although serious enforcement proceedings have yet to occur. The Act establishes a strong punishment system, with fines of up to ₹250 crores (about €27.5 million) for crimes such as data breaches, lack of valid user permission, and disregard for individual data rights. The Act demonstrates India's intention to construct a preventative and deterrent regulatory paradigm, with a heavy emphasis on data fiduciary accountability, consent-driven data processing, and rigorous monitoring of third-party data processors. [10]

With its extensive rights and strong enforcement procedures, the GDPR continues to be the world standard for data protection. However, it has issues with uniform implementation among EU member states, slow enforcement, and heavy compliance requirements for SMEs. By giving customers rights over their personal data, the CCPA represents a major advancement in U.S. privacy legislation; yet, in comparison to the GDPR, its state-level reach and weak enforcement make it a more disjointed and less unified framework. By establishing robust data rights and penalties, India's Digital Personal Data Protection Act, 2023, is a significant step forward. However, its efficacy will rely on the independence of the proposed Data Protection Board of India and the clarity of future regulations, especially with regard to ensuring checks on government surveillance powers and fostering institutional trust.

3. Role of AI in Data Collection, Processing & Analysis

Artificial intelligence (AI) systems, such as virtual assistants and LLMs, gather enormous volumes of personal data, from voice and behavior patterns to location and biometrics. This data collection is frequently heightened by ongoing surveillance through mobile applications and the Internet of Things. Sensitive profiling—where AI extrapolates personal information such as political opinions or medical issues from neutral data—is made possible by this extensive data collecting, increasing the possibility of predicting damage.

AI incorporates automated data management tools—tagging, encryption, and anomaly detection—to identify breaches and flag critical material in order to reduce these risks. Secure, decentralized AI training is made possible by privacy-preserving methods like homomorphic encryption, federated learning, and differential privacy, which guarantee that raw personal data is safeguarded at the source.

4. AI and Data Privacy: Potential Benefits vs Risks

4.1 AI's Contribution to Improving Data Security and Privacy

AI greatly improves data privacy through effective data processing, compliance assistance, and automated threat detection. Instant breach detection is made possible, data management is structured and compatible with laws (such as the DPDP Act and GDPR), and anonymization techniques are used to support tailored services. By simplifying risk assessments, bias checks, and legal compliance under frameworks like the EU AI Act and Colorado AI Act, AI also improves governance, supports granular user controls like ethical auto-redaction, and improves consent management. [11]

4.2 Possible Privacy Concerns with AI

AI presents a number of privacy issues, such as the possibility of prejudice and discrimination in delicate domains like credit or law enforcement, as well as widespread surveillance and profiling without authorization. In black-box systems, opaque decision-making compromises accountability and transparency. Furthermore, AI that collects too much data raises the possibility of abuse and increases the susceptibility to security breaches. [12]

5. Ethical Considerations in AI-Driven Data Practices

Important ethical concerns are brought up by AI, including deepfakes that violate consent, loss of user control (such as the inability to enforce the "right to be forgotten"), and opaque decision-making. Furthermore, skewed training data might reinforce societal injustices, and autonomous choices and excessive energy use raise questions about sustainability and responsibility.

The following are some best practices for reducing these risks:

- **Embedding bias checks, PETs, and encryption** early in system design for built-in privacy and security.
- **Using Explainable AI (XAI)** to ensure decisions are understandable and traceable.
- **Strengthening vendor governance** with strict transparency and consent protocols for third-party AI systems.
- **Promoting AI literacy and training**, especially aligned with frameworks like the **EU AI Act**.
- **Establishing cross-functional oversight** through multidisciplinary committees to regularly audit AI systems and enforce ethical compliance.

6. Emerging Threats: Cyber Fraud

Cyber fraud is the use of the internet or digital technology to defraud individuals or organizations for financial gain, data theft, or other nefarious intent. With the rising digitization of services and reliance on online platforms, cyber fraud has emerged as one of the world's most urgent cybersecurity issues.

Types of Cyber Fraud

There are several ways that cyber fraud might appear. The most common and harmful kinds are as follows:

(i) Phishing

Phishing is a type of fraud in which criminals send false emails, messages, or websites posing as trustworthy organizations (such as banks, social media sites, or governmental organizations) in an attempt to fool users into disclosing private information like credit card numbers, login credentials, or personal information.

Variants: Spear phishing is targeted phishing directed at certain people or companies. Whaling: Attacks directed against governmental authorities or high-ranking executives. Vishing and Smishing: Phishing using phone calls (vishing) or SMS (smishing). For example, in a cryptocurrency fraud in 2020, hackers compromised the Twitter accounts of prominent public personalities (such as Elon Musk and Barack Obama) via spear phishing emails. [13]

(ii) Theft of Identity

Identity theft is the process by which a hacker utilizes stolen personal identifying information (PII), such as PAN cards, Aadhaar numbers, or Social Security numbers, to pretend to be the victim in order to carry out fraudulent activities or get benefits.

Techniques: Breach of data Phishing infections caused by malware

For example, the 2018 Aadhaar data leak in India, which revealed the personal information of more than 1 billion people, caused grave worries about the possibility of identity theft. [14]

(iii) Fraud in Online Banking

This is breaking into a person's or company's bank account without authorization in order to steal money or perpetrate financial fraud. To get around two-factor authentication, phishing, malware, or SIM switching are frequently used.

Typical Methods: Software for keylogging, Trojan horses False, banking websitesn, As an example, the Jamtara phishing scam in India revealed how small-town scammers tricked individuals out of their bank passwords and OTPs by using phony calls. [15]

(iv) Fraud Using Credit Cards

Fraudsters conduct illegal internet transactions using credit card information that has been stolen. This information can be obtained by Breach of data Devices for skimming E-commerce sites that were breached

As an example, the Domino's India data breach in 2021 revealed the delivery addresses and credit card information of 18 crore orders. [16]

(v) Attacks Using Ransomware

Malware that encrypts a victim's files and requests a ransom to unlock them is known as ransomware. People, companies, and even public infrastructure are targeted by it. Notable strains include Maze, REvil, and WannaCry. For example, the 2017 WannaCry ransomware assault, which targeted the government, financial, and healthcare industries, compromised over 200,000 machines in 150 countries.

(vi) Email Compromise in Business (BEC)

In this scam, hackers impersonate or breach top executives' email accounts in order to approve fictitious money transactions or fool staff members into disclosing private information.

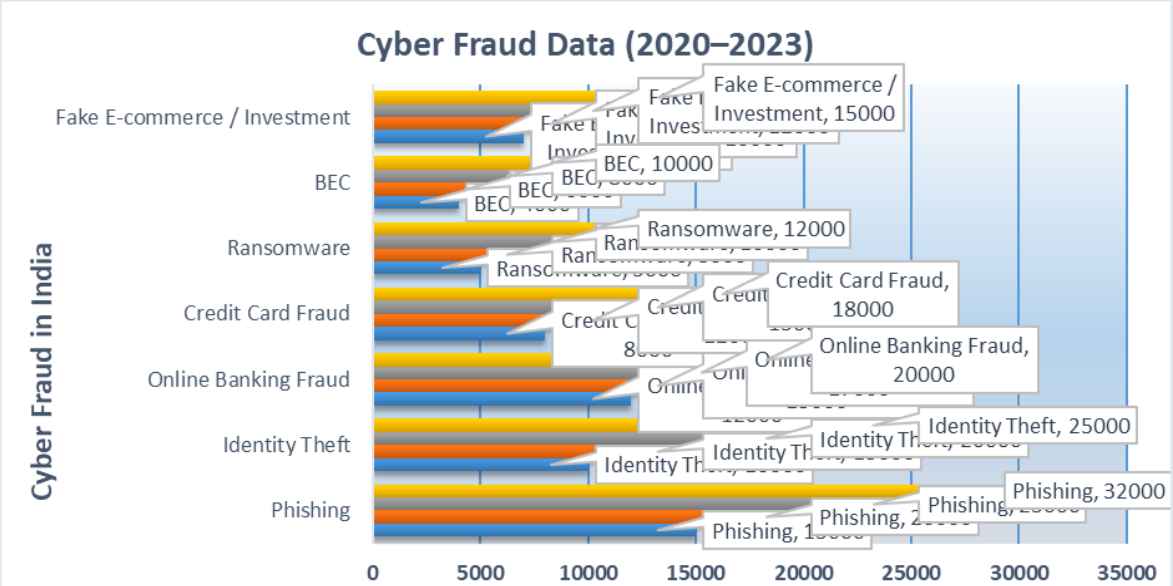
As a case study, in 2016, a BEC fraud cost an Austrian aerospace company more than €50 million. [17]

(vii) Fake Investment and E-Commerce Websites

Cybercriminals make phony websites or applications that seem like trustworthy online retailers or investment portals, frequently promising speedy returns or too-good-to-be-true offers.

Warning Signs: No safe channel for payments, Absence of client support, No contact details that can be verified, In particular, the GainBitcoin scam in India defrauded investors out of more than ₹2,000 crore through fraudulent bitcoin investments. [18]

Here's a column chart of cyber fraud trends from 2020 to 2023, including phishing, identity theft, and ransomware.



	Phishing	Identity Theft	Online Banking Fraud	Credit Card Fraud	Ransomware	BEC	Fake E-commerce / Investment
2023	32000	25000	20000	18000	12000	10000	15000
2022	25000	20000	17000	15000	10000	8000	12000
2021	20000	15000	15000	12000	8000	6000	10000
2020	15000	10000	12000	8000	5000	4000	7000

Sources: Cyber fraud trends in India are chiefly tracked by three major organizations.

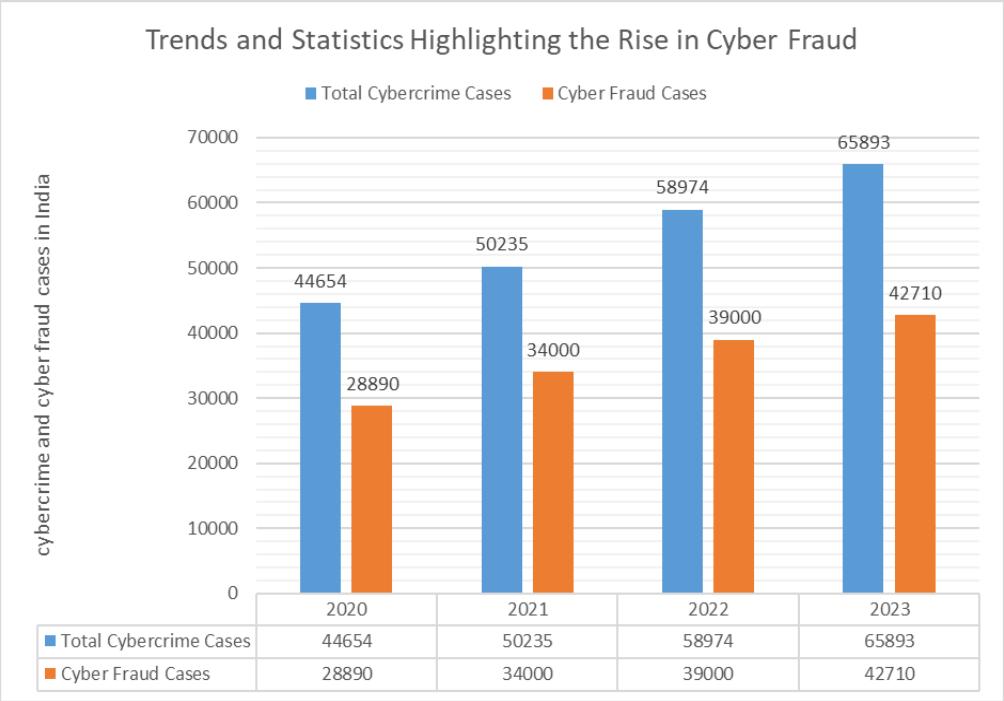
The **National Crime Records Bureau (NCRB)** provides official annual statistics through its *Crime in India* report, which recorded 65,893 cybercrime cases in 2022—64.8% of which were fraud-related (NCRB Report, PIB Summary). The **Indian Computer Emergency Response Team (CERT-In)** monitors real-time threats such as phishing and ransomware, logging 13.9 lakh incidents in 2022 and 15.9 lakh in 2023 (CERT-In Reports, Press Release). The **Data Security Council of India (DSCI)** offers sector-specific threat intelligence, such as in its India Cyber Threat Report 2023. Additional context and real-world impact are highlighted in **Norton Cyber Safety reports** (noting that 1 in 3 Indians faced cybercrime in 2023), and media outlets like *The Indian Express*, *Times of India*, and *Hindustan Times*, which provide case-based coverage.

7. Trends and Statistics Highlighting the Rise in Cyber Fraud

Due to low digital literacy and high digital use, cyber fraud continues to rise in India. Over 65,000 cybercrime cases were reported, with online fraud and identity theft accounting for a significant portion of these cases, according to the NCRB Crime in India Report 2022. The

increasing danger landscape is reflected in the more than 14 lakh cybersecurity incidents that CERT-In recorded in 2023. These statistics are supported by the 2023 Norton Cyber Safety Insights Report, which discovered that 1 in 3 Indians have been victims of cybercrime, primarily financial theft. According to these data, India is among the top 5 nations in the world for cyber fraud.

The following column chart shows the patterns of cybercrime and cyberfraud incidents in India between 2020 and 2023:



Sources: Key statistics on cyber fraud and security concerns in India and across the world are gathered from a variety of credible sources. The NCRB's "Crime in India" reports (2020-2023) (ncrb.gov.in) provide annual statistics on cybercrime crimes, notably fraud-related events. CERT-In's annual reports (cert-in.org.in) monitor real-time cybersecurity risks including phishing and ransomware. The RBI's yearly reports (www.rbi.org.in) show developments in digital payment fraud. On the consumer side, the Norton Cyber Safety Insights Report (in.norton.com) exposes the scope of individual-level cyber dangers in India. Globally, reports from Interpol (interpol.int) and Europol's IOCTA (europol.europa.eu) provide insights into transnational cybercrime patterns and growing threats.

8. Proposed Reforms and Enhancements in Data Privacy, AI Regulation, and Cybersecurity

8.1 Data Privacy: Established Laws & Recent Amendments

India

- The DPDP Act, which was enacted on August 11, 2023, will go into effect on January 1, 2025, and grants people the right to access, amend, remove, or withdraw their consent. It also forbids the behavioural profiling of children and imposes fines of up to ₹250 crores (~$30 million) on cross-border transfers.

United States (state-level patchwork)

- Virginia (VCDPA), Colorado (CPA), Utah (UCPA), Tennessee, Florida, Montana, and other states passed privacy legislation with GDPR-style protections, opt-outs, and breach reporting in 2023–2025.
- In 2025, California revised the California Privacy Rights Act (CPRA), adding stricter limits for automated decision-making and increasing the criteria for income.

Asia Middle East

- Israel's 1981 Privacy Law was amended in August 2024 with Amendment No. 13, which went into effect in August 2025.
- Australia and Malaysia: Australia passed the Privacy Amendment Act in December 2024 with fines increased to A$50M and an expanded offshore scope; Malaysia updated its PDPA in 2024–2025 (e.g. breach reporting within 72 hours, DPOs, portability); etc.
- Indonesia put its own PDPL into effect in October 2024, while the UAE and Saudi Arabia did the same in 2022, with enforcement stepping up by September 2024 The law in Vietnam will go into effect on January 1, 2026.

8.2 Artificial Intelligence Regulation: From Guidelines to Laws

EU AI Act (Regulation 2024/1689)

- Adopted in March–May 2024, the application went into effect on August 1st, 2024, and was phased in over a period of 6–36 months, depending on the risk class (e.g., high-risk obligations up to 36 months; prohibitions on unacceptable-risk applications after 6 months).
- AI systems can be categorized as unacceptable, high-risk, limited, minimum, and general-purpose; they are subject to penalties (up to 7% of worldwide turnover), transparency, documentation, human oversight, and conformance evaluations.

The European AI Board, AI Office, and national agencies coordinate enforcement among member states.

United States

- No federal AI law yet; more than 45 states have advanced over 550 AI-related bills addressing AI in areas like privacy, safety, and liability
- Recent "AI Action Plan" (July 2025) under President Trump aims to deregulate AI, remove federal references to DEI and misinformation in NIST guidelines, limit state-level regulation, accelerate infrastructure, promote AI exports, and deny federal contracts to models that fail ideological neutrality standards.

Asia-Pacific & Other Regions

- Canada: A principle-based framework called Proposed Bill C-27 (AIDA) calls for risk assessment, accountability, and transparency for AI systems.
- China: Since 2023, rules have been implemented to combat generative AI, deepfakes, and disinformation; AI systems are subject to stringent labeling and transparency requirements. In December 2024, South Korea passed a legally enforceable Basic AI Law that went into effect in January 2026 and used a risk-based approach.
- The Model AI Governance Framework (2019), which was revised in January 2024 for generative AI and included concepts of accountability, justice, and openness, was pioneered by Singapore.
- South Africa, Japan, Thailand, Australia, and Turkey: Various attempts, including strategy papers, ethics principles, and national guidelines, but typically no legally enforceable legislation as of yet.

8.3 Cybersecurity: Convergence of New Laws & Strengthened Regulation

European Union

- Adopted in January 2023, the NIS 2 Directive (Directive 2022/2555) requires risk management, incident reporting, and stricter enforcement for essential and significant entities throughout the EU. It is implemented through national legislation, such as Ireland's National Cyber Security Bill 2024, and imposes fines of up to €10 million, or 2% of global revenue, on essential entities.
- Adopted in October 2024 and going into effect in December 2027, the Cyber Resilience Act (CRA, Regulation EU 2024/2847) established broad cybersecurity obligations for products with digital components, such as required security upgrades and incident notification.

- DORA, or the Digital Operational Resilience Act: Enforced as of January 17, 2025, and centered on the banking industry and ICT third-party service providers, it ensures operational resilience in the face of digital disruptions.

United Kingdom

- The Cyber Security and Resilience Bill (CS&R), which was unveiled in July 2024, would bring the UK's NIS 2018 into compliance with EU NIS 2 and establish tighter regulatory authority and standards for reporting ransomware. Information on enforcement is currently being developed.

- **Australia**

Under Australia's 2023–30 Cyber Security Strategy, the Cyber Security Bill 2024 was passed in November 2024. It creates a Cyber Incident Review Board, requires the reporting of ransom payments, and specifies cybersecurity requirements for consumer smart devices.

9. CONCLUSION

Artificial intelligence (AI), extensive data ecosystems, and rising cybercrime pose a serious threat to established data privacy standards. This article examines how AI-driven technologies have surpassed the regulatory capabilities of traditional legal frameworks, especially with regard to consent, accountability, transparency, and algorithmic bias. Even if laws like the CCPA, GDPR, and India's DPDP Act, 2023, have established fundamental rights and safeguards, their application, enforcement, and flexibility in response to the ever-changing digital environment are still inconsistent.

Furthermore, a complex regulatory approach is required due to AI's dual nature as a source of new risks and a solution for improved data security. Ethical conundrums like profiling, data abuse, spying, and the loss of personal freedom highlight how urgent it is to incorporate privacy and security by design into AI development and governance. Growing instances of cybercrime throughout the world, particularly in India, underscore the practical repercussions of legislative deficiencies and a lack of public knowledge.

10. REFERENCES

1. King, Jennifer and Caroline Meinhardt, (2024). Rethinking Privacy in the AI Era. Retrieved from: https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf and accessed on 20 May, 2025 at 9:05am.
2. Retrieved from: https://www.taxmann.com/post/blog/overview-of-digital-personal-data-protection-act-dpdp-act and accessed on 21 May, 2025 at 8:10am.

3. Digital Personal Data Protection Act, 2023**,** Sections 6 to 8.
4. Retrieved from: https://lawctopus.com/clatalogue/clat-pg/digital-personal-data-protection and accessed on 12 Jun, 2025 at 11:05am.
5. Online Available at https://www.noandt.com/en/publications/publication20230928-2 and accessed on 24 June, 2025 at 9:30am.
6. Retrieved from: https://airacle.in/blog/dpdp-act-2023-explained/? and accessed on 20 May, 2025 at 9:05am.
7. Online Available at https://www.taxmann.com/article/meta-fined-1-2-billion-euros-for-violating-gdpr-on-data-transfers/ and accessed on 26 June, 2025 at 10:05pm.
   Retrieved from:
8. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Fines_and_penalties and accessed on 02 July, 2025 at 8:36pm.
   Online Available at
9. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Fines_and_penalties and accessed on 07 July, 2025 at 9:05am.
10. Retrieved from: https://www.cookiehub.com/ and accessed on 08 July, 2025 at 11:05pm.
11. Retrieved from: https://blog.synergyit.ca/the-impact-of-ai-on-data-privacy-and-security-in-2025/ and accessed on 12 July, 2025 at 8:35pm.
12. Online Available at https://trustarc.com/resource/data-privacy-age-ai-whats-changing
13. Department of Justice, USA. "Three Individuals Charged for Alleged Roles in Twitter Hack." 2020.
14. The Tribune. “Rs 500, 10 minutes, and you have access to billion Aadhaar details.” Jan 4, 2018
15. India Today. “Jamtara Scam: India's Phishing Capital.” October 2020.
16. Economic Times. “Domino’s India data breach: 18 crore orders’ info leaked.” May 2021.
17. BBC News. “Email scam costs Austrian firm nearly €50 million.” March 2016.
18. Times of India. “GainBitcoin scam: ₹2,000 crore fraud using fake crypto promises.” Aug 2022.
19. Retrieved from: https://www.cookiehub.com/blog/the-india-digital-personal-data-protection-dpdp-act-2023? and accessed on 16 July, 2025 at 9:05am.
20. Online Available at https://lawctopus.com/clatalogue/clat-pg/digital-personal-data-protection-act/. and accessed on 27 July, 2025 at 10:05am.