



# Regulatory Challenges of Cybersecurity and Privacy: A Threat to Digital Economy

Prof. (Dr.) Tabrez Ahmad<sup>1</sup>, Zoha Tabrez\*<sup>2</sup>, and Aasma Warsi<sup>3</sup>

<sup>1</sup> Founding Dean and Head, MANUU Law School, Maulana Azad National Urdu University, Hyderabad, India [tabrezahmad7@gmail.com](mailto:tabrezahmad7@gmail.com)

<sup>2\*</sup> First-year BBA LLB student at: SVKM's NMIMS Kirit P. Mehta School of Law, Hyderabad, Jadcherla, Telangana, India [zohatabrez5@gmail.com](mailto:zohatabrez5@gmail.com),

<sup>3</sup> Consultant, CD&OE, Maulana Azad National Urdu University, Hyderabad, India [asmatabrez@gmail.com](mailto:asmatabrez@gmail.com),

## Abstract

Privacy & cybersecurity have become important pillars of fast growing digital space, as expanding cybercrimes like hacking, phishing, identity theft and ransomware pose severe risks to individuals, businesses, and governments. With global cybercrime costs expected to grow to \$1.2 to \$1.5 trillion annually by Dec 2025, strong legal and technological safeguards are needed. Cyberlaw provides the framework to secure transactions, protect data and enhance trust in online interactions by solving issues of data privacy, digital ethics and protection of intellectual property.

The **Digital Personal Data Protection (DPDP) Act, Information Technology (IT) Act, 2000**, and regulations from RBI, SEBI, and CERT-In provides the core of the legal landscape. The **Aadhaar Act (2016)** and **BNS 2023**, alongside policies such as the **National Cyber Security Policy**, further enhance e-governance & data protection.

As the AI, IoT, and global connectivity further expanding the cyber threats to grow in scale and sophistication. A comprehensive frameworks for cyber awareness, threat intelligence, and data protection are becoming very critical. Cyber laws thus serve as the foundation for a secure, ethical, and resilient digital ecosystem. It further required to balance innovation with safety in the expanding digital economy.

**Keywords:** “Cybersecurity, Privacy, Cybercrime, Digital landscape, Digital ethics”

## 1. Introduction:

Cybercrime is defined as the criminal activities carried out through use of digital devices or computers networks. It is generally divided into 3 categories.<sup>1</sup> **Cybercrime** with individuals; targets individuals to steal their personal data or invade their privacy (for e.g., cyberstalking, hacking, identity theft ). **Cybercrime** against property; Attacks financial systems or digital assets (for e.g., phishing, ransomware, data breaches) & DOS attacks. **Cybercrime against the Government**; posing serious security threats the nation by stealing classified data & disrupt operations of the Govt. institutions. Cybercrime is growing by leaps and bounds and in-fact it has grown **600% since the pandemic**; re-emphasising as the protection & awareness essential.

**1.1 Common types of cybercrimes:<sup>2</sup> AI-powered attacks:** It use artificial intelligence for phishing, adaptive malware & data manipulation. Insider threats: Employees misusing internal access for sabotage & theft. Cyberterrorism; attacks on critical infrastructure such as power grids or governments. Computer vandalism; destroying or corrupting data using ransomware or viruses. Malware & ransomware; infecting systems to steal, encrypt, or destroy data. Cross-site scripting (XSS); injecting malicious code into trusted websites. Cyber harassment & stalking: Bullying, threatening, or tracking individuals in cyberspace. Copyright infringement; illegal use or distribution of copyrighted contents.

Denial-of-Service (DoS/DDoS); overcrowding of servers for disruption of access.

Online defamation; uploading & promoting false or harmful content about others.

Exploitation & human trafficking; sing online platforms for illegal activities.

Drive-by & eavesdropping attacks; infecting devices or intercepting data via unsecured networks. Phishing; fake emails or sites that steal sensitive data.

Understanding these cybercrimes and having proper regulatory standards with the supported technological developments are the key in building safer digital habits and defending against evolving online threats.

---

<sup>1</sup> <https://cuetolawgroup.com/types-of-cybercrime/>, visited on 19<sup>th</sup> Feb, 2025

<sup>2</sup> <https://www.lawctopus.com/academike/recent-developments-in-cybersecurity-law-challenges-and-opportunities/>, visited on 18<sup>th</sup> Feb, 2025

## 2. Cybersecurity Regulation Challenges<sup>3</sup>

Cybersecurity regulations face several challenges due to evolving technologies, global data exchange, and diverse legal frameworks.

**Emerging Technologies;** AI, IoT, and blockchain raise privacy, ethics, and regulatory gaps. **Cross-Border Data Transfers;** different national laws cause compliance issues in international data movement (e.g., GDPR, Privacy Shield). **Employee Awareness;** human error remains a top security threat; maintaining regular training is crucial. **Incident Response;** varying breach notification laws complicate response planning.

**Regulatory Penalties;** non-compliance can lead to heavy fines and reputational harm.

**Privacy by Design;** integrating privacy in early product stages remains challenging.

**Consumer Rights;** ensuring transparency and handling user data requests efficiently.

**Data Minimization;** difficulties in limiting and managing data retention for analytics-driven firms. **Third-Party Risks;** vendors handling sensitive data must meet compliance standards and undergo audits. **Cyber Insurance;** organizations struggle with policy clarity and meeting insurer requirements.

## 3. The Laws Enacted to Safeguard Privacy and Combat

### Cybercrime.<sup>4</sup>

There are various laws enacted to safeguard the Privacy and Control of Cybercrimes as follows:

#### 3.1 General Data Protection Regulation (GDPR) – EU (2018)

The GDPR is a well-defined EU law that fixed data privacy across Europe and gives individuals good control on their private information. It is applicable to all organizations affecting EU citizens' data, also outside the EU.<sup>5</sup>

The essential points of this law is that it Grants rights such as data access, correction, deletion (“right to be forgotten”), and portability. It requires explicit, informed user consent for data processing. It mandates appointment of Data Protection Officers (DPOs) for oversight. Its non-compliance can provide to fines ranging from to €20 million or 4% of global turnover.

---

<sup>3</sup> <https://lawfullegal.in/cybersecurity-legal-frameworks-challenges-and-the-role-of-law-in-protecting-digital-assets>, visited on 20<sup>th</sup> Feb, 2025

<sup>5</sup> <https://blog.ipleaders.in/digital-personal-data-protection-act-dpdpa-2023>, visited on 22<sup>nd</sup> Feb, 2025

Strengths: It is a very strong data protection, international influence, empowers users and creates accountability.

Weaknesses: It has very high compliance cost, jurisdictional issues, operational complexity, & uneven enforcement.

### 3.2 California Consumer Privacy Act (CCPA) – USA (2020)

The CCPA provides privacy rights & consumer protection for California residents. It enhances users control on how their personal data is used, collected & shared.<sup>6</sup> It provides specific points like right to know, delete, and opt-out of personal data sales. Rights of Non-Discrimination to protects users exercising privacy rights. The rights of transparency in businesses to disclose data practices.

Expanded by California Privacy Rights Act (CPRA) in 2020 for stronger protections.

**Strengths:** Boosts consumer rights, transparency, and fairness.

**Weaknesses:** It includes only data exemptions, & have weak enforcement mechanisms also Limited to California only.

### 3.3 Information Technology Act, 2000 (IT Act)

The IT Act, 2000 is India's first law regulating cybercrime, digital transactions e-commerce & m-commerce. It is enforced on 17<sup>th</sup> October, 2000, provides legal recognition to electronic signatures, digital records fixed the legal base for online business & e-governance.<sup>7</sup>

The Act provides a Cyber Appellate Tribunal to resolve disputes and a Controller of Certifying Authorities for overseeing electronic signatures. It has further amended the Indian Penal Code and Evidence Act to include the cyber offences.

Key provisions include:

- **Section 43A:** provides compensation for failure to protect data.
- **Section 66C:** provides identity theft.
- **Section 66B:** provides punishment for receiving stolen digital property.
- **Section 66E:** criminalises privacy violations.

The 2008 Amendments included specific regulations on voyeurism cyber terrorism, pornography, and child exploitation, in association with Section 69 (government power

<sup>6</sup> Rob Bonta, <https://oag.ca.gov/privacy/ccpa>, visited on 21<sup>st</sup> Feb, 2025

<sup>7</sup> Anju S. Nair Critical Assessment of Information Technology Act, 2000.

<https://corpbiz.io/learning/critical-assessment-of-information-technology-act-2000/>, visited on 23<sup>rd</sup> Feb, 2025

to intercept communications). The Section 66A, was struck down by the Supreme Court in 2015 as un-constitutional since the said section penalized “offensive messages,” for violating freedom of speech & expression.

**3.4 Subordinate Rules are the Intermediary Guidelines Rules (2011) and Digital Media Ethics Code (2021)** regulate social media and digital platforms.

#### **3.4.1 Strengths:**

- Legal recognition for e-documents and signatures.
- Framework for tackling cybercrimes.
- Enables e-governance and corporate cyber protection.
- Establishes redressal mechanisms like the Cyber Appellate Tribunal.

#### **3.4.2 Weaknesses:**

- Incomplete coverage of new cybercrimes (e.g., cyberstalking, fraud).
- Lacks robust **privacy and data protection** measures.
- Weak enforcement and implementation.
- Does not address **intellectual property** or **domain name** issues.

### **3.5 Digital Personal Data Protection Act, 2023 (DPDP Act) & Draft Rules, 2025**

The **DPDP Act, 2023** is India’s first comprehensive **privacy and data protection law**, governing the processing of **digital personal data**—both online and offline (if digitized). It also applies to entities outside India that process data related to offering goods or services in India.<sup>8</sup>

The Digital Personal Data Protection Act, 2023 (DPDP Act) was introduced in the Lok Sabha on August 3, 2023, passed on August 9, and enacted on August 11, 2023. The Draft Rules, 2025 were released on January 3, 2025, for consultation till February 18, 2025. Written in simple, inclusive language using “she” instead of “he,” the Act promotes gender equality.

It is applicable to all personal data except publicly available information and is consent-based model. Therefore it requires explicit, informed consent for processing. Data Fiduciaries are required to define the purpose, security of data retention. The Significant Data Fiduciaries (SDFs) required to appoint a Data Protection Officer, who conduct audits, and perform functions of impact assessments. The various penalties ranges from ₹10,000 to ₹250 crore, fixed by the Data Protection Board of India (DPBI). Emerged

---

<sup>8</sup>The Digital Personal Data Protection, <https://thelegalschool.in/blog/data-privacy-act-india>. Visited on 13/02/2025

in the 2017 K.S. Puttaswamy judgment. the DPDP Act promotes privacy as a fundamental right.

The Draft Rules, 2025 emphasize clear notice and consent procedures, consent management through registered managers, stronger security and breach reporting measures, and a defined framework for cross-border data transfers to ensure better data protection and accountability.

The **DPDP Act, 2023** is **user-centric and consent-based**, ensuring accountability of data fiduciaries and enforcement through the **Data Protection Board of India (DPBI)**. It promotes transparency and has global applicability to protect Indian citizens' data. However, it faces challenges like **broad government exemptions, unclear cross-border data rules, limits under the RTI Act, and implementation difficulties for SMEs**.

### **3.6 National Cyber Security Policy, 2013:**

This Indian policy emphasises creating a secure and resilient cyberspace. It encourages on protecting critical information infrastructure, ensuring cybersecurity awareness, and pushing law enforcement agencies to have comprehensive framework. It further promotes collaboration between sectors, and enhanced cyber readiness. But it has implementation challenges, limited resources, evolving threats, and gaps in public awareness.

### **3.7 Cybersecurity Information Sharing Act (CISA):**

This United States law encouraging private & public partnership in cyber threat intelligence. It enhances voluntary information sharing, protects interests of participating organizations, and provides privacy protection while information exchange.

### **3.8. Network and Information Security (NIS) Directive:**

There is EU directive which enhances cybersecurity by asking the member states to promulgate national cybersecurity strategies, appoint national authorities to report various cybercrimes.

### **3.9 Cybercrime Prevention Act:**

This law criminalizes cybercrimes such as identity theft, hacking, and cyber fraud, putting rigorous penalties and imprisonment which is being adopted by various countries like Philippines etc.

Together, these frameworks aim to strengthen cybersecurity, safeguard digital systems, and protect personal privacy in an evolving global cyber landscape.

#### 4. Conclusion:

Data privacy & cybersecurity have taken the centre stage for safety, innovation & trust. The exponential expansion and sophistication of cybercrimes from AI-driven attacks, phishing, & ransomware requires well-built technical, & legal set-up. International regulations like the CCPA GDPR, NIS Directive, India's IT Act 2000, National Cyber Security Policy 2013, DPDP Act 2023 essentially form the cornerstone of ethical & sure digital environment.

However, effective governance of cybersecurity & robust regulation with continuous adaptation, public awareness and international cooperation is a must. As technical growth emerging through IoT, cloud computing & AI, laws must ensure agility to bridge the gaps between regulation & innovation. Businesses, individuals & Government must share responsibility by investing in threat intelligence, design practices to ensure privacy & digital literacy.

As the resilient cyberspace depends on harmonizing privacy, economic growth & security. By global collaboration, cooperation & empowering citizens with legal rights, and ensuring liability in data security, internationally we can build a safe, trustworthy & inclusive cyberspace to protect individual freedoms, liberty & sustainable digital culture, business, trade & economy.

#### References:

1. Bada, A., & Sasse, M. A. (2015). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre, University of Oxford*.
2. Cybercrime Prevention Act of 2012, Republic Act No. 10175 (Philippines).
3. Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501 et seq. (United States).
4. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (California, USA).  
California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq. (California, USA).
5. Digital Personal Data Protection Act, No. 22 of 2023. (2023). *Gazette of India*, Ministry of Law and Justice. Retrieved from <https://www.meity.gov.in/>

6. Draft Digital Personal Data Protection Rules, 2025. (2025). *Ministry of Electronics and Information Technology (MeitY), Government of India*.
7. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, L 119/1.
8. Information Technology Act, 2000 (India). (2000). *Gazette of India, Ministry of Law, Justice and Company Affairs*. Retrieved from <https://www.meity.gov.in/>
9. Information Technology (Amendment) Act, 2008 (India). (2008). *Gazette of India*.
10. K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
11. National Cyber Security Policy, 2013. (2013). *Ministry of Electronics and Information Technology (MeitY), Government of India*.
12. Network and Information Security (NIS) Directive, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1.
13. Privacy Shield Framework. (2016). *European Commission and U.S. Department of Commerce*.
14. OECD. (2021). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation*. Paris: OECD Publishing.
- UNODC. (2020). *Global Cybercrime Report*. United Nations Office on Drugs and Crime.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

