Page 1827 - 1846 **DOI:** *https://doij.org/10.10000/IJLMH.118698*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

© 2024 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **Gyan@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Online Privacy and Cybersecurity: Regulations and Challenges

SHWETANG RAJENDRA DANEKAR[1] AND AJIT KAMBLE[2]

ABSTRACT

Cyber security has become crucial to any nation's security, economy, and overall well-being. While much has been written about India's rise as a global computing power, not much is known about its cyber security history. This paper examines the critical importance of online privacy and cybersecurity in the digital age. It provides an overview of key concepts related to online privacy, including data collection, usage, security, and user consent. The paper compares online privacy regulations in India, the United States, and Russia. It then analyzes major challenges to securing online privacy in India, such as lack of comprehensive data protection laws, government surveillance concerns, and low digital literacy. Common threats to online privacy like weak passwords, oversharing on social media, and IoT device vulnerabilities are discussed. The paper reviews key Indian legislation aimed at protecting online privacy and preventing cyber threats, including the Information Technology Act 2000, IT Rules 2021, and the Digital Personal Data Protection Act 2023. It also examines cybersecurity challenges like evolving threats, skills shortages, and rapid technological change. The paper concludes by comparing cybersecurity penalties in India to other countries and emphasizing the need for robust, forward looking laws to address emerging cyber risks in an increasingly digital world.

***Keywords**: Data protection, Digital literacy, Cyber threats, Privacy regulations, Data security.*

I. INTRODUCTION

As online data handling becomes more prevalent, online privacy and cybersecurity should be viewed as closely linked entities. The security of personal information, whether in transit or stored, now heavily relies on organizations implementing robust cybersecurity measures to safeguard it effectively. In certain situations, cyber security protocols are put in place to safeguard critical infrastructure systems that protect sensitive data, thereby shielding personal information.

Protecting online privacy is crucial for safeguarding individuals' rights, particularly given the

[1] Author is a student at Manikchand Pahade Law College, Chh. Sambhajinagar, India.
[2] Author is a student at Manikchand Pahade Law College, Chh. Sambhajinagar, India.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

rapid shift towards a digitalized world, which brings numerous challenges and issues. To overcome these challenges, specific legislation, guidelines, and regulations are required to govern and manage them effectively. Dealing with online privacy and cybersecurity is also fraught with challenges, and establishing rules and regulations is necessary to address these issues.3

(A) What is online privacy?

The definition of online privacy is as follows:

According to the Cambridge Dictionary of Sociology, "privacy is closely linked to individualism as the private sphere, separate from the public realm, is meant to shield individuals from both social security and political observation".4

In the digital realm, online privacy is defined as the safeguarding of an individual's personal details and data when they are connected to the internet.

While viewing your preferred social media platform, you are literally isolated in a physical space. You are also subject to being observed or having your activities disrupted by others. You may be physically apart, but you are still visible on someone's screen. Furthermore, your viewing experience is frequently disrupted by advertisements that encroach on your videos, articles, and online browsing. The following information clarifies the aspect of online privacy for better understanding.

- **Data Collection:** Online services and websites collect various types of data about users, including their personal information, browsing habits, location data, and more.
- **Data Usage:** Once collected, data can be used for various purposes, such as targeted advertising, content personalization, or even sold to third parties.
- **Data Security:** Ensuring data security and protection against unauthorized access or data breaches is a fundamental aspect of online privacy.
- **User Consent:** Online privacy often involves the idea that users should have the choice and consent over what data is collected about them and how it is used. This includes both opt-in and opt-out mechanisms for data sharing.
- **Anonymity and pseudonymity:** User's ability to engage with online services and platforms without revealing their true identity is another component of online privacy.
- **Encryption:** The use of encryption technologies can help protect the privacy of

[3] Online privacy – Barkha and U Rama Mohan , cyber laws and crimes book.
[4] Cambridge dictionary of sociology – privacy and its importance.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

communications and data transmission over the internet, which makes it more challenging for unauthorized parties to intercept or access information.

- **Online Tracking:** Concerns regarding online tracking, including cookies and tracking pixels, are central to discussions of online privacy. Users may worry about being constantly monitored while browse the web.
- **Cybersecurity:** Ensuring the security of online activities is closely related to privacy. Cyberattacks, such as hacking and identity theft, can compromise personal information and online privacy.
- **Privacy Settings and Tools:** Many online services provide users with privacy settings and tools to manage their data and control who can access it.5

II. COMPARISON OF ONLINE PRIVACY IN INDIA AND SPECIFIED COUNTRY

India: - The concept of right to privacy was declared to be a fundamental right pronounced through a judgement by the Hon'ble Supreme Court of India. Data Protection in India has been a recent phenomenon developed over the years. There are no specific law or statue for Data Protection in India. However, they are indirectly mentioned in certain legislation.

For Instance, Article 21 of the Indian Constitution mentions on Right to Life and Personal Liberty. In 2017, the Right to Privacy was declared to be a fundamental Right under Article 21 of Indian Constitution. In case of any violation, a suit can by the individual under Article 32 of Indian Constitution.6

The Indian Penal Code has been into existence from the British Rule. The Indian Penal Code was mainly enacted to give punishments for the criminal offences within the premises of India. IPC does not specifically mention about directly However, IPC mentions about privacy concerns indirectly. It protects individuals whose privacy is violated. Section 471 of IPC mentions usage of electronic document which is forged, such person shall be punished in the same manner that of he forged.

Sec 379 of IPC mentions about theft any person who dishonestly takes into his possession without the owner's consent shall be punishable with imprisonment of three years or fine or both. Information Technology Act,2000- The Act was established to deal with all the Cybercrimes, any frauds, or complaints in e-commerce sector. The Act also establishes provisions for data protection and data privacy concerns. Furthermore, now digital personal data

[5] Data and Goliath : The hidden battles to collect your data and control your world – Bruce Schneier
[6] Constitution of india – Article 21 and Article 32.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

protection Act, 2023 came into force.

USA: America is considered to be the most developed, powerful and also resourceful country of the globe. They have also given recognition to Right to Data Privacy. They have specific laws enacted by their Parliament. Any person whose Data Privacy has been infringed can file a suit in the Court of Law. Suit can be filed for any data infringement and for the disclosure of personal and sensitive information to a third party without the owner's consent. There have been various amendments in the US Constitution to protect the rights of their citizens. Amendments have also been made with concern to Data Privacy. For instance, the fourth amendment of the US Constitution provides citizens with privilege to any arbitrary search and seizure by State Authorities. They also have separate Acts enacted for different purposes.7

Russia: The Russian Constitution also highlight on Right to Privacy on individuals it also recognizes it as a Fundamental Right similar to India. They have strict laws to protect the personal and sensitive laws of the three individuals where it mentions that no communication or transfer of data should be made without the consent of the owner.

However, there is an exception when data are collected by the state authorities. The consent of individuals plays a very significant role. Article 24 of the Russian Constitution specifically mentions the consent of the owners, no person shall collect, store, or publish any personal data without express consent of the owner. If done without consent, the operator will be held liable with imprisonment up to 2 years and fine up to 2,00,000 rubles.8

III. CHALLENGES IN SECURING ONLINE PRIVACY IN INDIA

Securing online privacy in India, like in many other countries, comes with its own set of challenges. These challenges arise from a combination of technological, legal, cultural, and economic factors. Here are some challenges to online privacy in India:

- **Lack of Strong Data Protection Laws:** India has historically lacked comprehensive data protection laws. While the Personal Data Protection Bill was introduced in 2019, it was not passed at that time by parliment, till the digital personal data protection Act, 2023 is came into force in India. But this Act is still not ready for the future cyberattacks. The absence of strong legal frameworks can lead to weaker privacy protections for individuals.(Now India have law called Digital Data Protection Act,2023)
- **Data Collection and Profiling:** Companies, government agencies, and other

[7] United States Constitution – Rights of privacy.
[8] Russian constitution – Article 24, Penalties for offences.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

organizations collect vast amounts of personal data in India. These data can be used for profiling, advertising, and other purposes, potentially infringing on individuals' privacy.

- **Government Surveillance:** There have been concerns about government surveillance in India, particularly with regard to the use of technologies like facial recognition and the interception of digital communications. These practices can infringe upon citizens' privacy rights.
- **Data Breaches:** Data breaches and cybersecurity threats are common in India and affect both government and private sector organizations. These breaches can expose sensitive personal information, putting individuals at risk of identity theft and other privacy violations.
- **Digital literacy:** Many Indians, especially in rural areas, have limited digital literacy. This vulnerability increases their vulnerability to online privacy threats, such as falling for phishing scams or sharing personal information unintentionally.
- **Social media and Online Harassment:** The widespread use of social media has led to online harassment and cyberbullying. These issues can affect the privacy and safety of individuals.
- **Inadequate Consent Mechanisms:** In many cases, individuals are not adequately informed about how their data will be used, and they may not have meaningful options to consent or opt out of data collection and processing.
- **Cross-Border Data Flow:** Data are often transferred across international borders, making it difficult to enforce privacy regulations, especially when dealing with multinational companies.
- **Biometric Data Usage:** The use of biometric data, such as Aadhar data, for identity verification, has raised concerns about the security and privacy of such data.
- **Cultural Factors:** Privacy is often seen differently in different cultures, and in some cases, there may be less highlight on individual privacy in India compared to Western countries. This can affect how people perceive themselves and protect their own privacy.

Companies often have economic incentives to collect and monetize user data, which can lead to privacy violations if not properly regulated.[9]

[9] Online privacy – Barkha and U Rama Mohan , cyber laws and crimes book

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

IV. THREATS TO ONLINE PRIVACY

(A) Weak and reused passwords

At some point or another, we all used weak passwords. Maybe you still do. It is not uncommon. But it is, however, one of the biggest threats to your privacy.

Reusing weak passwords is a leading cause of massive data breaches you see in the news. That is because it allows cyber criminals to break into multiple accounts at once and engage in identity theft or financial fraud, often both.

(B) Oversharing

Social media and other technological advancements have made it incredibly easy to share every aspect of our lives to expand our social ties. Oversharing is a consequence of that which often goes unnoticed because so many people do it.

Oversharing gives malicious onlookers more information about you than they would ever want to make known. Posting videos of your home gives them a full map of your belongings and how to get rid of them. Pictures of your boarding passes reveal how long you'll be gone and where you retraveling. Every post, you create a clearer picture of your life, habits, key relationships, and possessions.[10]

(C) IoT Devices (internet of thing devices)

Another threat to your online privacy: all the Internet-connected devices that constantly listen, record, and gathering data about you.

Our shopping lists, our body temperature, the contents of our fridge—we have been producing this personal data for years, but no one has been interested in it before. We now have connected toothbrushes, toasters, and TVs all over the place.

IoT devices are easy to use, and they keep improving, increasing the risks to your online privacy on the way.

(D) Unsecured Web Browsing

The browser is probably the most used app on your devices - consciously or not. Each time you open a link or run an online search; your default browser is one of the main ways to connect to the Internet. You may have even let it remember your passwords.

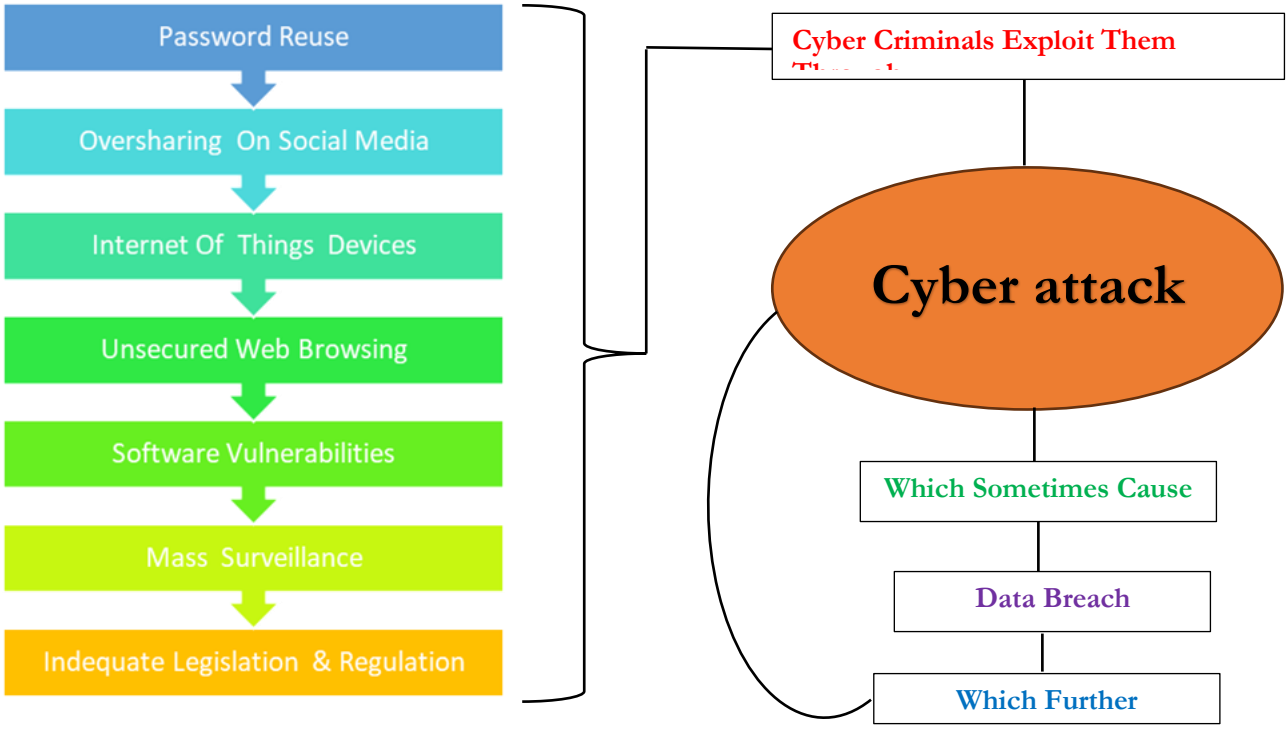
Cyber-criminals know that too! And they're going after everything in it through malicious

[10] Online threats – bitdefender.com

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

extension infected ads, links that lead to scam websites, and a lot more.

Security and privacy risks usually come as a combo. Besides cyber-crooks and scammers, companies can also build an accurate profile of you based on your browse history.



(E) Security Vulnerabilities

It is not just your habits and the mechanisms of platforms and devices you use that weaken your privacy on the Internet. Security vulnerabilities can also create significant issues. They range from data breaches, where a set of personal data is ultimately made publicly accessible places online, to security issues that make devices misbehave.

Security vulnerabilities leak data that hurt not only your personal privacy online but also that of millions of users which weakens the overall security level for all of us.

(F) Cyber-Attacks

Your online privacy has everything to do with your security when you are online.

Relying on default settings for everything and using the simplest passwords can make you an easy target for cyber criminals.

Malicious hackers combine their technical skills with psychological manipulation to exploit your habits and preferences so that you will click, tap, download, and open their traps.

V. RULES AND REGULATION MADE FOR ONLINE PRIVACY AND ITS PUNISHMENT IN INDIA

(A) Information Technology Act, 2000: - When this IT Act, 2000 came into force on October 17, 2000, all the laws and procedures in reference to the given Act lacked the protection and provisions required to protect one's sensitive personal information provided electronically. This eventually led to the introduction of the Information Technology Bill, 2006 in the Indian Parliament, which then led to the Information Technology (Amendment) Act, 2008 whose provisions came into force on October 27, 2009.

(B) It inserted Section 43A in the Information Technology Act: "a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected.

(C) Section 66E of Information Technology Act, 2000: -In the age of internet and social media, there is a risk of violation of privacy either by capturing and publishing images of private areas of any person by any person, which could feel humiliation. Therefore, to protect any person against such privacy violation, Section 66E was inserted in the Information and Technology Act, 2000. This gender-neutral section applies when any person's privacy is violated which provides for the harshest punishments together with fine.

(D) Section 66E: - It deals with punishment for any person who violates the privacy of any person. In case of violation of privacy by, intentionally or knowingly, capturing, publishing or transmitting the image of a private area of any person without his or her consent.[11]

(E) Punishment: He or she shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or with both.

VI. CASE LAWS

(A) Justice K. S. Puttaswamy (Retd.) & Anr. vs. The union of India & Ors. AIR 2017 SC 4161

[11] Information technology Act, 2000- section 43A, section 66E, Punishments

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

This case is the cornerstone of the 'Right to Privacy' jurisprudence in India. The nine Judge Bench unanimously reaffirmed the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was integral to freedoms guaranteed across fundamental rights and was an intrinsic aspect of dignity, autonomy and liberty.

The case began with the question of whether the right to privacy was a fundamental right, which was raised in 2015 in the arguments concerning the legal validity of the Aadhaar database.12

VII. CYBERSECURITY

Cybersecurity refers to the practice of protecting computer systems, networks, and data from theft, damage, unauthorized access, and other forms of digital attacks. It includes technologies, processes, and practices designed to safeguard information technology assets and ensure the confidentiality, integrity, and availability of data and systems.

India is in a position to become a global leader in terms of data, technology, digitalization and every field. The government has been also taking initiatives and giving green signals to programs like Startup India, Digital India etc. with the long-term aim to boost the environment for existing and new businesses to become global unicorns. India has significant potential for growth in the coming years. And as the digital economy grows, it becomes increasingly liable to cyber threats and vulnerabilities. For example, there is a growing risk of cyberattacks on key infrastructure as well as financial institutions.

Cybersecurity is incredibly important for new era people like us because it directly impacts our daily lives and the future. It's not just about protecting our social media accounts; it's safeguarding our personal information, financial assets, and even our personal information, financial assets, and even our future job prospects. As we navigate the digital world, strong cybersecurity habits will help us to avoid falling victim to scams, identity theft, and online harassment. In addition, in an increasingly tech-driven job market, understanding cybersecurity can open up exciting career opportunities. It is like having a superpower that keeps your digital life safe and can be a valuable skill in our personal and professional journey. 13

(A) Why cybersecurity is important?

The importance of cybersecurity is universally understood because cybersecurity is related to safeguarding valuable digital assets and personal safety. The following are the key points:

[12] Case laws - https://indiankanoon.org/doc/127517806/
[13] Introduction to Cyberseccurity – Ajay singh

a. **Protecting Personal Information**: Cybersecurity protects sensitive data, including financial records and personal details, from theft or misuse.

b. **Preventing Financial Loss**: This method guards against online fraud, identity theft, and scams that can lead to substantial financial losses.

c. **Privacy Preservation**: This step ensures that your online activities remain private, preventing unauthorized access or surveillance.

d. **Business Continuity**: For companies, cybersecurity is crucial to maintain operations, protecting data, and prevent disruptions caused by cyberattacks.

e. **National Security**: Governments rely on cybersecurity to protect critical infrastructure and sensitive data from cyber threats and espionage.

f. **Trust and Reputation**: Strong cybersecurity builds trust with individuals, customers, and partners, thereby preserving an entity's reputation.

g. **Legal Compliance**: Many laws and regulations require organizations to implement cybersecurity measures, and non-compliance resulting in legal consequences.

h. **Global Impact**: Cyber threats know no borders; therefore, strong cybersecurity is essential on a global scale to counteract digital risks.[14]

(B) **Cybersecurity: challenges**

Cybersecurity is of utmost importance in today's digitally connected world because cyberattacks can have several consequences, including financial losses, damage to reputation, and compromise of sensitive information. Organizations, government agencies, and individuals all play a role in maintaining a strong cybersecurity posture to avoid these risks. Cybersecurity faces a continuously evolving landscape of challenges and threats. Some prominent challenges that arise in the field of cybersecurity includes Cyberattacks, zero-day vulnerable. Insider threats and many more let us understand what are the challenges of cybersecurity.[15]

Certainly, here is a more detailed explanation of the key challenges in cybersecurity.

- **Evolving Threat Landscape:** Cyber threats continue to evolve in terms of sophistication and variety. Malicious actors develop new tactics, techniques, and tools, making it difficult to predict and defend emerging threats.

[14] The Indian Cyber Law by Suresh T. Vishwanathan
[15] Challenges to Internal security of India – Ashok kumar, Vipul anekant

- **Limited number of skilled professionals:** The demand for cybersecurity experts far exceeds the supply. This skill gap results in understaffed security teams and organizations struggling to find and retain qualified personnel.
- **Human Error:** Many cybersecurity breaches occur due to human error, such as falling for spam emails, misconfiguring security settings, and accidentally disclosing sensitive information. Educating individuals and employees about cybersecurity is a continuous challenge.
- **Rapid Technological Advances:** The pace of technological change, such as cloud computing, AI, and IoT, can outstrip an organization's ability to implement strong security measures, leaving vulnerabilities in newly adopted technologies.
- **IoT and BYOD:** (The increasing use of Internet of Things devices and the practice of "Bring Your Own Device") In workplaces expand the attack surface, making it more challenging to secure all entry points.
- **Data Privacy Regulations:** Complying with data privacy regulations like the Information technology Act, 2000 and data protection measures, adding complexity to cybersecurity strategies.
- **Supply Chain Vulnerabilities:** Attackers may exploit weaknesses in the supply chain, compromising hardware or software before it reaches end users. This highlights the need for thorough vetting of suppliers and ensuring the integrity of the supply chain.
- **Nation-State Attacks:** State-sponsored cyberattacks are a growing concern, with governments targeting critical infrastructure, organizations, and even other nations. Attacks can be highly sophisticated and politically motivated, posing significant threats.
- **Budget Constraints:** Many organizations struggle to allocate sufficient financial resources to cybersecurity. Limited budgets may result in insufficient protection, leaving systems vulnerable to attack.
- **User Awareness:** Despite awareness campaigns, users often underestimate cybersecurity risks and fail to follow best practices. Raising awareness and promoting a culture of security within organizations remains a persistent challenge.
- **Zero-Day Vulnerabilities:** Zero-day vulnerabilities are unknown software flaws that cybercriminals can exploit before developers release patches. Organizations must constantly monitor and adapt to emerging threats, even when there are no available fixes.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

Addressing these challenges requires a multi-faceted approach that combines technology solutions, continuous education, robust policies and procedures, and international cooperation to share threat intelligence and respond effectively to the evolving cyber landscape. In ongoing efforts to stay ahead of cyber threats and protect digital assets.16

(C) Role of Indian legislation to prevent cyber threats

Indian legislative has done very vital role to prevent the cyber threats and made some laws and acts to prevent. The following points will give deep dive of the role of Indian legislation to prevent cyber threats**:**

a. The Information Technology Act of 2000

India's first landmark cybersecurity law was the Information Technology Act

The IT Act of 2000 was enacted by the Parliament of India and was administered by the Indian Computer Cybersecurity Response Team (CERT-In) to guide Indian cybersecurity legislation, institute data protection policies, and govern cybercrime. It also protects e-governance, e-banking, e-commerce, and the private sector, among others.

Although India does not have an exclusive, unitary cybersecurity law, it uses information Technology IT Act and multiple other sector-specific regulations to promote cybersecurity standards. The framework also provides a legal framework for critical information infrastructure in India.

For example, in Section 43 of IT Ac, Indian businesses and organizations must have "reasonable security practices and procedures" to protect Sensitive Information from being compromised, damaged, exposed, or misused.

Under Section 72A of the IT Act, any intermediaries or persons that disclose personal data without the owner's consent (with ill intention and causing damages) are punishable by imprisonment of up to three years, a fine of up to Rs. 500,000, or both.

Intermediaries and body corporates to report cybersecurity incidents to CERT-In

- Preventing unauthorized/unlawful use of a computer system
- Protecting private data and information from DDOS cyberterrorism, attacks, phishing, malware, and identity theft
- Legal recognition of organizations' cybersecurity
- Safeguarding electronic payments and electronic transactions and monitoring and

[16] A Study of cybersecurity challenges and its emerging trends on latest technologies, G.Nikita Reddy1,

decryption of electronic records

- Establish a legal framework for digital signatures
- Recognizing and regulating intermediaries17

b. **IT Rules, 2021**

On February 25, 2021, the Ministry of Electronics and Telecommunication introduced the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, as a replacement for IT Rules, 2011. A little over a year later, on June 6, 2022, the newly updated draft amendments were published by the Indian MeitY (Ministry of Electronics and IT) to improve the IT Act to keep up with the challenges of the ever-changing digital landscape.

The new amendments aim to allow ordinary users of digital platforms to seek compensation for their grievances and demand accountability when their rights are infringed upon, as well as institute additional due diligence on organizations.

IT Rules, 2021 also distinguishes between smaller and more significant social media intermediaries based on user numbers and places a much heavier burden on larger social media intermediaries concerning personal data protection.

In addition, there are changes to the privacy and transparency requirements of intermediaries, such as:

- It requires intermediaries to inform users about rules and regulations, privacy policy, and terms and conditions for usage of its services
- Requiring intermediaries to designate a grievance officer who can address and resolve user complaints about violations of IT Rules, 202118

c. **KYC (Know Your Customer)**

KYC (Know Your Customer) processes are standards and practices used worldwide and mandated by the RBI (Reserve Bank of India). KYC is the tracking and monitoring of customer data security to improve the safeguard against fraud and payment credential theft. It requires banks, insurance companies, and any other digital payment companies to conduct financial transaction to verify and identify all of their customers.

For proper KYC compliance and financial regulatory requirements, businesses need to include

[17] The Information Technology Act, 2000, Ministry of Electronics and Information Technology, Government of India.
[18] IT Rules, 2021

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

the following cybersecurity steps:

- Having a knowledge-based questionnaire test to verify customer identities
- Implement prescreening KYC verification methods like email verification, phone verification, Device ID intelligence, and reputational data, among others
- Using AI-based technology and machine learning to verify documents and government-issued IDs
- Using biometrics like fingerprinting and facial recognition, to verify a user's identity
- Maintain a customer database for verification19

Businesses with KYC policies assure customers that they have relevant compliance management and anti-fraud solutions to protect their digital identities and payment transaction data. With KYC Compliance, Indian merchants can have peace of mind with safe and secure payment processing, complying with regulations from SEBI, as well as establishing trust with customers. Failing to adhere to KYC guidelines, banks, businesses, and corporations may face a monetary penalty of ₹2 lakh (₹200,000).

d. **Reserve Bank of India Act 2018**

The Reserve Bank of India introduced the RBI act in 2018, which provides cybersecurity guidelines and frameworks for UCBs (urban co-operative banks) and payment operators.

The RBI Act of 2018 aims to:

- Create standards that equalize banks and payment operators' security frameworks according to how they adapt to new technologies and digitalization.
- Mandate banks to create and present crisis management plans.
- Mandate banks to implement corporate-approved (board-approved) information security policies that will successfully outline cybersecurity preparedness.
- Requires banks to implement mandatory breach notifications, in which UCBs must promptly detect and report cybersecurity incident to RBI within 2-6 hours of discovery to better respond to the attacks. In addition, encourage banks to regularly schedule threat assessment audits.
- Help banks implement their email domains using anti-pacing and anti-malware technology, as well as enforce DMARC security controls.

[19] Reserve Bank of India, Cyber Security Framework for Banks, (2016).

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

All Indian banks must follow these guidelines to standardize frameworks for payment processing cybersecurity and combat the ever-increasing business complications that emerge in a digital environment. The RBI Act of 2018 imposes fines on banks and the financial sector in cases of non-compliance with cybersecurity requirements. The penalty can be up to ₹10 lakh (₹1,000,000).20

e. The Digital Personal Data Protection Act of 2023 (DPDP)

On August 11, 2023, the President of India signed the "The Digital Personal Data Protection Bill" following its approval from both houses of the Indian Parliament. This enactment establishes a dedicated legal framework in India, marking a significant milestone in India's first-ever privacy Act that has been designed to regulate the processing of digital personal data, acknowledging both individuals' right to safeguard their personal information and organizations legitimate purposes for data processing.

A data protection law has been in place since 2017, when the Supreme Court, in the landmark Puttaswamy judgement, ruled that privacy is a fundamental right of Indian citizens, putting the government under the obligation to pass legislation to protect this right. The Act allows the free transfer of personal data outside India, except for countries expressly restricted by the Central Government.

Applicability: The Bill applies to the processing of digital personal data within India where such data is: (i) collected online or (ii) collected offline and is digitized will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.

Consent: Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. A notice must be given before seeking consent. The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Consent will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.

Rights and duties of data principal: An individual whose data is being processed (data

[20] Reserve Bank of India Act, 2018, cybersecurity guidelines and framework for UCB.

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

principal), will have the right to: (i) obtain information about processing, (ii) seek correction and erasure of personal data, (iii) nominate another person to exercise rights in the event of death or incapacity, and (iv) grievance redressal. Data principals will have certain duties. They must not: (i) register a false or frivolous complaint, and (ii) furnish any false particulars or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.

Transfer of personal data outside India: The Bill allows transfer of personal data outside India, except to countries restricted by the central government through notification.

Data Protection Board of India: The central government will establish the Data Protection Board of India.21

(D) **Penalties**

1. Failure to prevent personal data breach (sec.5(8)): Up to INR 250 crore
2. Failure to notify the board and data principals (sec.5(6)): Up to INR 200 crore.
3. Non-fulfillment of obligations while processing children's data (sec.9): Up to INR 200 crore.
4. Non-fulfillment of obligations by a significant data fiduciary (sec.10): Up to INR 150 crore.
5. Breach of any voluntary undertaking given to the Board (sec.32): Penalty up to the extent applicable for the breach.
6. Miscellaneous non-compliance with provisions of the Act: Up to INR 50 crore22

VIII. THE PUNISHMENT OF CYBERSECURITY IN INDIA CAMPARE TO OTHER COUNTRIES

The punishment for cybersecurity-related offenses in India and other countries, varies significantly depending on the nature and severity of the offense, the applicable laws, and the specific circumstances of the case. It's important to note that I cannot provide real-time or up-to-date information on specific penalties because laws can change and vary by jurisdiction. However, I can offer a general comparison of how punishments for cybersecurity offenses may differ between India and some other countries:

[21] The Digital Personal Data Protection Bill, 2022. [16] Torsha Sarkar, "The Legal Challenges to India's Proposed Surveillance Regime", (2019) 54(25) Economic and Political Weekly.
[22] Digital personal Data protection Act, 2023/penalties.

(A) India: In India, the punishment for cybersecurity offenses can range from fines to imprisonment, depending on the specific offense and the provisions of the Information Technology Act, 2000.

- For unauthorized access to computer systems, data, or networks, punishment may include imprisonment up to three years or a fine.
- If an offense results in damage to a computer system or data, punishment may include imprisonment up to three years and a fine.
- For more severe offenses, such as hacking with the intent to cause harm or data theft, penalties can be more severe, including longer prison terms.[23]

(B) United States- In the United States, penalties for cybercrime are outlined in various federal and state laws. Penalties include fines, probation, and imprisonment.

- Federal laws like the Computer Fraud and Abuse Act (CFAA), provide for imprisonment and fines for unauthorized access, computer intrusions, and related offenses.
- Punishments can vary widely depending on the specific cybercrime and its impact, with sentences ranging from months to several years or more.[24]

(C) European Union (EU):

- The European Union has stringent data protection laws, such as the General Data Protection Regulation (GDPR), which can result in substantial fines for organizations that mishandle personal data.
- Cybersecurity-related offenses can also be subject to criminal penalties under national laws in EU member states, with fines and imprisonment as potential sanctions.[25]

IX. CONCLUSION

In the modern technology era, daily new cyber threats arises and for that to protect individuals' Online privacy we need strong laws, and that laws also need amendments by taking consideration of future cyberattacks because every single day new technology came into existence. In the Indian judiciary the Justice Chandrachud will introduce the Online Court system and for that this new law is going to help in Indian judicial system for privacy and confidentiality of an individuals. Cybersecurity is about the insecurity made by and through this

[23] Information technology Act, 2000/ Digital personal data protection Act,2023
[24] Computer Fraud and Abuse Act (CFAA)
[25] General data protection regulation (GDPR)

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

new space and about the practices or procedures to make it (progressively) secure. efforts to verify the cyberspace should give a definite need else the "information technology" will not be directly used by clients.

For every powerful and modern country, strong cybersecurity is required for the welfare of the country and it emerges any country in the world of technology. Internet online things is increasing because every work is now online, we need to secure our data, privacy, from cyber criminals such as hackers etc., for that cybersecurity laws are there. But The law should be future ready.

*****

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

X. BIBLIOGRAPHY

- Online privacy – Barkha and U Rama Mohan , cyber laws and crimes book.
- Data and Goliath : The hidden battles to collect your data and control your world – Bruce Schneier
- Constitution of India – Article 21 and Article 32
- US constitution – Right to privacy
- Russian constitution – Article 24 and penalties for offences
- Online threats – bitdefender.com
- Case laws - https://indiankanoon.org/doc/127517806/
- Introduction to Cyberseccurity – Ajay singh
- Challenges to Internal security of India – Ashok kumar, Vipul anekant
- National Cyber security Policy
- DPDP Act 2023
- IT Rules, 2021
- The Information Technology Act, 2000
- The Indian Cyber Law by Suresh T. Vishwanathan
- A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES G.NIKHITA REDDY1 , G.J.UGANDER REDDY2
- https://www.thehindu.com/sci-tech/technology/80-indian-companies-hit-cybersecurity-incidents-miscommunication-it-team-kaspersky-report/article66535520.ece
- Section 43A, The Information Technology Act, 2000.
- Justice K.S. Puttaswamy(Retd) v. Union of India, (2017) 10 SCC 1.
- The Personal Data Protection Bill, 2019.
- The Information Technology Act, 2000, Ministry of Electronics and Information Technology, Government of India.
- The Information Technology (Amendment) Act, 2008, Ministry of Electronics and Information Technology, Government of India.
- Reserve Bank of India, Cyber Security Framework for Banks, (2016).

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]

- Reserve Bank of India, Framework for securing Card Transactions, 2022
- Department of Telecommunications, Guidelines for Telecom Service providers regarding National Security related information, (2011).
- The Digital Personal Data Protection Bill, 2022. [16] Torsha Sarkar, "The Legal Challenges to India's Proposed Surveillance Regime", (2019) 54(25) Economic and Political Weekly.
- Computer Fraud and Abuse Act (CFAA)
- Gerneral Data Protection Regulation (GDPR)
- Dennis, Michael Aaron, Cybercrime, Encyclopaedia Britannica, (19 Sep. 2019), https://www.britannica.com/topic/cybercrime.
- Henry et al, Countering the Cyber Threat, 3 no. 1 The Cyber Defense Review, 47–56 (2018).

*****

© 2024. International Journal of Law Management & Humanities [ISSN 2581-5369]