INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

EVOLVING CYBERSECURITY AND DATA PROTECTION FRAMEWORKS: GLOBAL REGULATIONS AND INDIA'S LEGISLATIVE DEVELOPMENTS

AUTHORED BY - PAWNI MISHRA

Abstract

This is a major global issue as speed of digital transformation in enterprises is increasing. The Internet of Things (IOT), cloud computing, and artificial intelligence (AI) have been rapidly developing and with them have appeared new threats that can be exploited by hackers with the help of ransomware, malware, phishing and social engineering. There is a need for strong cybersecurity and data protection frameworks to leverage in order to protect sensitive information, corporate operations and national security This paper aims at exploring the progressive cyber threats and evaluates the current legal frameworks to address them. Even the global regulations such as the GDPR and the CCPA have provided a reference for data privacy. The cybersecurity governance in India is still developing. India's cybersecurity governance is also a developing area, despite the IT Act, 2000 and the recently proposed Digital Personal Data Protection Bill (DPDPB), 2023, to regulate cybercrime and data security. However, there are still weaknesses in enforcement, missing regulations on cross border data flow and lack of adequacy of the current laws to the new age cyber threats. The paper also examines the role of corporate cybersecurity policies, international cooperation, and new technologies in cyber risk management. The paper further notes that managing insider threats, ransomware attacks, and APTs needs compliance with the regulations, the awareness of cybersecurity, and the ability to detect threats. Moreover, cyber resilience strategies, PPPs and dynamic legal systems are very vital in enhancing the national cyber security postures. This research also provides insights on strengthening India's cybersecurity policy by evaluating the existing security laws, regulatory concerns, and global best practices. This report points out the need for Congress to take proactive legislative action, the need for more funding for cybersecurity research and the need for international cooperation to fight successful future cyberattacks. It is crucial for policies to combine legal, technological, and organizational mechanisms to ensure a safe online framework.

 ISSN: 2582-6433

Keywords: Cybersecurity, data protection, cyber threats, ransomware, phishing, social engineering, GDPR, IT Act 2000, Digital Personal Data Protection Bill, AI-driven cyberattacks, insider threats, cyber resilience, regulatory compliance, cybersecurity governance, international cooperation.

Introduction

In today's world of globalization, virtual architecture cannot exist without cybersecurity. As technology advances and globalization is happening at an unprecedented rate, there is a requirement for protecting personal information, sensitive data, and important systems. This is important as protecting valuable systems and sensitive data becomes more significant. Cyber security in the sense of safeguarding networks, data, and devices from cyber-attacks and unauthorized access is needed to shield companies and individuals from monetary loss, national security threats, and damage to their reputation. With the rise of cyber-attacks like malware, ransomware, phishing, and DDoS, the difficulties of the digital world have increased. As these threats are targeted at computer systems and networks, it will be applicable to businesses and confidential details will be disclosed. Cyber threats become more malicious in an age where technologies like cloud computing, IoT, and AI are adopted more widely. The popular definition of cybersecurity is how to prevent unauthorized access, cyberattacks, and data breaches on networks, devices, and data. It is significant in that it will be able to shield individuals, companies and governments from attacks on the internet that expose profits and reputations and national security. As per the analysis up until October 2023 shows incident such as malware, ransomware, phishing and other attacks like DDoS reflect the growing complexities in the virtual world. The cyberattacks are taking a toll on operations, effectively invading people's personal data through vulnerabilities in the computer networks and systems. With the growth in cloud technology, artificial intelligence, and Internet of Things, the complexities that will be imposed in cybersecurity attacks will make them much different from previous forms of attack. With this new era of digitization, the biggest concern of all the world's nations is information privacy and safety. The implementation of strict cybersecurity regulations must be prioritized because data volume grows while its value heightens thus leading to increased asset importance. Data protection legislation from governments now exists in the form of the General Data Protection Regulation (GDPR) by the EU and the California Consumer Privacy Act (CCPA) in the United States and the Digital Personal Data Protection Bill in India and additional similar initiatives that clarify personal data usage and storage procedures. The 2000 IT Act in India has, primarily, the responsibility of cybersecurity, serving

 ISSN: 2582-6433

as the legal aspect of concerns about data security and anti-cybercrime. In the context of evolving cyber threat, there is an urge to tighten the existing legislation, enhance their more rigorous enforcement and increase acquaintance in the public and among companies. This research analyses key areas of cybersecurity in a new direction in terms of types of cyber threats and topics such as data security and international cybersecurity law. It also stresses the need for India to strengthen its legal framework and technology controls to counter more effectively new cyber threat trends.

Research Objectives

1. The evaluation of data protection legislation serves to preserve personal information alongside sensitive data from irresponsible access and misuse and cyber dangers.
2. This research investigates how Indian data protection laws developed through IT Act, 2000 and Digital Personal Data Protection Bill, 2023 while analysing their success in protecting against cybersecurity problems.
3. The examination of data protection protocols in India utilizes international standards of GDPR, CCPA and PIPEDA to discover current deficiencies and upcoming modernization areas.
4. The evaluation research analyses the Digital Personal Data Protection Bill 2023 by identifying its beneficial aspects as well as its weaknesses and its consequences on companies alongside citizens and police agencies.
5. The evaluation targets the enforcement systems and regulatory compliance concerns about data protection laws that exist in India.
6. The objective is to build data protection recommendations for India's legal framework which will match modern cybersecurity threats alongside international standards of practice.

Research Methodology

The research methodology implements a doctrinal interpretation with qualitative and analytical methods to analyse the cybersecurity laws and data protection systems of India. Researchers who use the doctrinal approach must read statutes, cases and legal principals which govern cybersecurity and data protection. This research analyses primary materials beginning with the Information Technology Act, 2000 plus its amendments with their related case laws in order to establish what laws apply to the subject. Additional evaluation comes from the examination of

 ISSN: 2582-6433

books alongside articles, reports and expert perspectives which provide extensive comprehension of the discussed topic. The research adopts a qualitative method to decode official documents combined with shifting cybersecurity vulnerabilities and emerging technologies. The study depends on a thorough examination of existing laws alongside their operational effectiveness instead of using quantitative information. An analytical method serves to evaluate the advantages and disadvantages of present cybersecurity laws in India. The research evaluates the legal weaknesses together with the challenges in police enforcement and the effectiveness of existing laws against phishing attacks and ransomware incidents along with data protection issues. The study incorporates international best practices and their findings to make improvement suggestions. The research uses doctrinal, qualitative and analytical strategies to perform a comprehensive and analytical examination of India's cybersecurity and data protection laws to identify weaknesses and improvements.

Hypothesis

1. Modern cybersecurity threats along with privacy concerns receive inadequate protection from Indian data protection laws which consist of both the IT Act 2000 and the Digital Personal Data Protection Bill 2023.
2. Insufficient enforcement mechanisms together with incomplete regulatory oversight make data protection laws in India less effective for public use.
3. The data protection regulations of India fail to achieve GDPR and CCPA global standards which creates complicated legal situations and additional compliance obstacles.
4. The Digital Personal Data Protection Bill, 2023 contains essential reforms yet lacks sufficient privacy security because it maintains general government exceptions and imprecise interpretations.
5. India will boost its cybersecurity posture and data privacy standards through a complete regulatory structure and clear execution procedures and international partnerships between countries.

CYBERSECURITY

Networks and computers together with utilities and private data receive Défense from threats and unauthorized access through cybersecurity practices. Protecting data and communication networks from unauthorized access as well as modification or exploitation defines the scope of

 ISSN: 2582-6433

cybersecurity. The defensive technology of computers and information systems operates under the name of IT Défense. The protective measures of cyber security defend both physical systems along with digital infrastructure and computer networks as well as data storage facilities from harmful attacks or invasion attempts. Network protection occurs through cybersecurity which represents a technological system to defend networks against such attacks. All possible threats and weak points affecting a computer system or network are encompassed within its considerations. The system proceeds with solution implementation after discovering its key weaknesses which guides the security measures to protect it. Under the provisions of the IT Act cybersecurity represents every effort to stop criminals from accessing or modifying data or computer hardware or communication devices and their associated data. Criminals use computer networks and communication systems for their offenses according to the National Cyber Crime Reporting Portal which serves as the government's complaint reporting system for cybercrime. The Internet of Things (IoT) gives rise to new security challenges since it keeps developing at an unprecedented pace. Cyberspace is regularly the target of several kinds of attacks that can result in a variety of disasters. The risk varies from minor to significant. We need to understand the kind of hazards that cyberattacks spread in order to combat them.[1] The following are a few of the several kinds of cyberattacks:

Malware

Users knowingly allow malware programs to impede their computer systems or other types of systems. The software has the capability to steal important information from users including banking details and password credentials. Such a program has the potential to steal valuable data, including bank account details and passwords. Moreover, the program can manipulate system settings and automatically open pop-up ads. Some common ones are computer viruses, worms, Trojan horses, ransomware, and spyware along with many other destructive programs. Since malware is highly dangerous to systems, it is vital for users and establishments to have understanding of assorted sorts of malware and take preventive measures, including the usage of antivirus programming, refreshing frameworks and applications, and being cautious when opening email connections or downloading programs from the cyber web. Malware is designed to harm and take advantage of your system or network. Its impact can be from slowing down your system to stealing sensitive data such as credit card numbers and passwords, or even giving hackers unauthorized access to your system. For example, there are spyware that follow

[1] Tanmay Vashishta, Cybersecurity and Legal Ramifications: An Important Concern in India, 2 INDIAN J. INTEGRATED RSCH. L. 1 (November-December 2022).

 ISSN: 2582-6433

your behaviour and report to an attacker, and there is ransomware that lock files on your system and the attacker will charge you a fee to unlock them. Laying the foundation for an upcoming attack is the first step; malware infection has the potential of spreading to devices on the same network. These risks can be mitigated, by keeping your antivirus tool up to data, and exercising caution when you click on links or attachments.

Ransomware

Ransomware is a type of malicious software that renders files on a person's computer or an organization inaccessible. Cyber attackers demand payment to decrypt the files. They understand that paying the ransom is often the easiest solution for the organization to retrieve its files, they have a counter advantage. In fact, there are variations with data theft being an additional way to pressure ransomware victims to make ransom payments.

Man in Middle

The Man-in-the-middle (MitM) attack is a particular kind of cyber-attack in which a third party secretly intercept and possibly alters the communication between two parties who believe they are directly communicating with each other. Since the attacker listens in on the conversation, the entire exchange can be manipulated. MitM attacks pose a significant threat to internet security because sensitive information like credit card numbers, account details, and passwords can be intercepted and manipulated in real-time.

Phishing

Phishing attacks involves fraudulent messages that appears to come from a trusted source. Most often, these types of attacks are conducted through email. Victims' computers can be infected with malware, or personal data usernames and passwords, credit card numbers and the like can simply be stolen. Everyone should be aware of phishing, as it is a common type of cyber-attack . The first step in phishing is sending a fraudulent email or similar type of message to target the victim. The message is crafted to look like it came from someone you trust. If the victim fails for the scam, they are often redirected to a fake website where they unknowingly share personal information

Distributed Denial of Services

Distributed denial of service attacks differs significantly from regular denial of service attacks. DoS attacks are carried out by someone using a single Internet connection to either take

 ISSN: 2582-6433

advantage of a software flaw or bombard a target with fictitious requests, generally in an effort to deplete server resources (such as CPU and RAM). Conversely, distributed denial of service (DDoS) attacks is initiated from a number of interconnected devices dispersed over the Internet. Due to there are large number of devices involved; it is significantly more challenging to mitigate these attacks. In contrast to single-source DoS attacks, DDoS attacks often aim to overload the network infrastructure with massive amounts of traffic. DDoS attacks can also be unique in the method used to accomplish them. Generally, attackers use botnets-large network of compromised devices (routers, PCs, cell phones) infected with viruses that allow an assailant to control them. On the other hand, denial of service attacks is typically launched using custom scripts or DoS tools.[2]

Cyber Security LAWS IN INDIA:

The expansion of computer usage has led to a proportional increase in the risk of unauthorized access and misuse. To regulate improper practices, the Indian government has introduced various legislations. Some of them are listed below:

1. **Draft Electronic Commerce Act of 1998[3]**: This act was presented to facilitate the creation of secure means for electronic commerce regulation via legal policies of digital signatures and other areas of electronic transactions. The Act came into existence to govern electronic contracts, provide security for e-transactions, and uphold the integrity of electronic data. It gives a legal framework to digital signatures, electronic transactions, and other issues concerning digital business.
2. **INFORMATION TECHNOLOGY ACT. 2000[4]:** The creation of the Ministry of Information Technology was made possible by this Act. The Indian government enacted this law in 2000 with the sole intention of making electronic transactions through information exchanges legal. Electronic data exchange, as well as other forms of electronic communication, became a standard practice in processing data, all being called electronic commerce. This process encompasses different methods of data storage and communication. The Act also makes it easier to file electronic documents with government departments. It also addresses amendments to the BNS, BSA BNSS

[2] Badadare, Vidya & Patil, Rajashree & Waghmare, Dr. Vishal. (2018). Cyber Security Need of Digital Era: A Review. International Journal of Computer Applications. Volume 182 – No. 22. 9-12.
[3] Draft Electronic Commerce Act , 1998
[4] Information Technology Act, 2000

 ISSN: 2582-6433

3. **The Information Technology Amendment Act, 2008**[5]: This brought in necessary amendments to provide greater data privacy and more stringent and effective legislation. One of the key provisions of this law was the enlargement of India's territorial jurisdiction to include foreign users who commit unlawful acts from overseas. This Act brings international criminals within the purview of jurisdiction for committing offenses under Indian law and prescribes life imprisonment for child pornography. The Act also covers electronic governance and other important legal matters. It gives legal validity to electronic records and electronic signatures, making them valid in government operations and official transactions. The Act also brought changes to the Cyber Regulations Appellate Tribunal, rechristening it the Cyber Appellate Tribunal and making its regulatory mechanism more robust. The Tribunal was created to deal with cyber offense cases and provide efficient legal remedies.

Data Protection

Data protection is processes, guidelines, and legislations designed to protect sensitive information regarding individuals from unauthorized access, misuse, and loss. Responsible handling of data is a requirement for the individual, corporate, and organizational sectors to perform data protection to ensure confidentiality and integrity in addition to meeting legal and regulatory requirements. Protection of data is achievable through methods such as encryption, access control techniques, and safe storage data technology, which protects data against unauthorized intrusion, theft, and hacking. An apparatus with data minimization, limitation of purpose, and accountability enforces strict data collection, storage, processing, and transmission rules. Furthermore, security programs that incorporate electronic transaction protections with cyber threat. Défense systems aid in preserving confidence and supporting legal systems to secure vital information in the modern information-based society.[6]

NEED FOR DATA PROTECTION

Data protection is a vital part of cybersecurity because individual records form precious digital data. The onset of worldwide technological advancements has turned data into a valuable resource, resulting in heightened cybercrime. The growth of data production surpasses a trillion bytes every year, with billions of devices connected that produce this much every year, as

[5] The Information Technology Amendment Act, 2008
[6] Prachi Chaudhary, Cyber Security Threat and Its Laws in India, 2 LAW ESSENTIALS J. 68 (2021).

 ISSN: 2582-6433

indicated by available studies, which estimate the growth will continue. Several nations have laws regarding cybersecurity; yet, several other nations need more comprehensive security laws. In the United States, cybercrime legislation is enforced under the Computer Fraud and Abuse Act[7], while the UK has the Computer Misuse Act 1990[8]. For India, the law governing cybercrimes is the Information Technology Act of 2000[9], along with The Bhartiya Nyaya Sanhita, 2023.[10] The legal limits of IT laws become ambiguous due to the lack of penalties in certain sections of the IT legislation framework. Online-assisted crime, including online-assisted murder, remains ambiguous in terms of classification under traditional criminal law or IT law. With the growing utilization of cloud computing and mobile phones, hacking cases are on the rise globally. In spite of India's advancement through its IT legislation, the international community needs to speedily enhance data protection mechanisms in order to deal efficiently with upcoming cybersecurity threats.[11]

INDIA'S CURRENT STATUS

According to the Data Protection Committee Report under Justice B. N. Srikrishna, it states, Article 21 of the Constitution offers fundamental privacy rights which emerge from that provision first and foremost. Article 21 of the Constitution[12], in Justice K.S. Puttaswamy (Retd) v. Union of India. To make this the state must establish a data protection framework as it bears responsibility to make this right operative. The state is obliged to ensure data protection services that shield citizens from informational privacy risks coming from state and non-state actors. The framework put in place by the state to protect personal data from state and non-state actors will benefit the broader population. On December 11, 2019, The Minister of The Minister of Electronics and Information Technology Mr. Ravi Shankar Prasad brought forward the Personal Data Protection Bill 2019 to Lok Sabha on December 11, 2019. Data Protection Bill, 2019[13] on Lok Sabha. The essential function of the Bill involves creating safeguards which protect personal data. The Bill works to safeguard personal data of individuals through the establishment of a Data Protection Authority. The parliament has not approved this piece of legislation. Different Indian legislations provide necessary protection when there is no complete single legislative act. Information Some surveillance power regarding the matters

[7] Computer Fraud and Abuse Act of 1986
[8] Computer Misuse Act 1990
[9] Information Technology Act of 2000
[10] The Bhartiya Nyaya Sanhita, 2023
[11] S. Ashwath, Importance of Data Protection, 1 JUS CORPUS L.J. 176 (June-August 2021).
[12] The Constitution of India 1950, Article 12
[13] Data Protection Bill, 2019

 ISSN: 2582-6433

exists through the enforcement of Information Technology Act along with the Telegraph Act. According to the previous explanation these regulations must not substitute an all-encompassing data legislation. the current scenarios. The Information Technology (Intermediary Guidelines and Digital Parliament approved the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on February 25th 2021. A new system of officers at these platforms would help increase their online security and privacy measures. Chief Compliance Officer and Grievance Compliance Officer. These rules replaced the Information Technology (Reasonable security practices and sensitive personal data or information) Rules, 2011. The Guidelines were established as drone usage became popular among people. drone operators now obtain permissions from the Directorate General of Civil Aviation (DGCA) according to Drone Rules, 2021[14] which separates drones by weight categories. A flight permission comes from DGCA to the pilot before operating a drone.[15]

DATA PROTECTION AND PRIVACY LEGISLATION WORLDWIDE

Computer usage expansion has led to a proportional rise in the possibility of its unauthorized use. Various acts came into existence as a means for the Indian Government to regulate improper practices. Some of them are stated below:

General Data Protection Regulation [16]serves as EU legislative control for personal data transfers beyond EU and European Economic Area territories starting from May 25, 2018 Through its implementation the GDPR provides EU citizens with greater authority to manage their personal information.

The CCPA represents a comprehensive state-wide data privacy law which established Californian consumer protection and privacy[17] rights since its June 28, 2018, promulgation. The California Privacy Protections Act (CPRA)[18] received voter approval in 2019 and established a November 4, 2020 enforcement date for modern consumer privacy rules within the state and its applicable industry regulations and enforcement systems. The CCPA will vanish from existence once the CPRA establishes its authority starting on January 1, 2023. Organisations need only reasonableness when using PDPA to manage personal data according

[14] Directorate General of Civil Aviation (DGCA) according to Drone Rules, 2021
[15] Rishi Nandhan R. B., Need for Data Protection Laws in India, 2 JUS CORPUS L.J. 72 (August 2021).
[16] General Data Protection Regulation, 2016
[17] Californian consumer protection and privacy, 2018
[18] The California Privacy Protections Act (CPRA), 2020

 ISSN: 2582-6433

to the 2012 Singaporean law.

The Personal Information Protection and Electronic Documents Act (PIPEDA)[19] establishes rules regarding personal data control by Canadian organizations for collection use and disclosure purposes.[20]

Initiative in India

Security against certain infractions pertaining to computer system data is guaranteed by this statute. Unauthorised use of computers, computer systems, and data stored on them is prevented by its restrictions. The Information Technology (IT) Act of 2000, as revised periodically, regulates all actions pertaining to the utilisation of computer system resources. All "intermediaries" involved in the usage of digital records and computer resources are also included.

The Information Technology (Intermediaries Guidelines) Rules, 2011[21] outlined the intermediaries' function in detail. As per the IT Act 2000, intermediaries:
Web hosting platforms, social media, telecom service providers, network service providers, and Internet service providers are examples of intermediaries as described in Section 2(1)(w)18 of the IT Act 2000. Additionally, it consists of search engines, online payment systems, online marketplaces, online auctions, online stores, and even cyber cafés. Anyone who looks after an electronic record on behalf of someone else is included. Importance of intermediaries under the law: For a specific amount of time, intermediaries are required to keep and control specific information in a format and manner defined by the Centre. The penalty for breaking this clause is three years in jail and a fine. By guaranteeing access to the resource in question, the middleman and any person in control of a computer resource should offer technical help. If this help is not given, the offender faces a maximum sentence of seven years in jail and a fine.

In the case of Shreya Singhal v. Union[22] of India, the Supreme Court interpreted the IT Act's provision stating that intermediaries should only take action after being notified in writing that a court order has been passed requesting that they specifically remove or disable access to a

[19] The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000
[20] Rishi Nandhan R. B., Need for Data Protection Laws in India, 2 JUS CORPUS L.J. 72(August 2021).
[21] The Information Technology (Intermediaries Guidelines) Rules, 2011
[22] AIR 2015 SUPREME COURT 1523

 ISSN: 2582-6433

particular piece of information.[23]

Digital Data Protection Bill

The recently proposed Digital Personal Data Protection law is a piece of legislation that delineates the rights and responsibilities granted to citizens (Digital Nagrik) as well as the responsibilities of different data fiduciaries while collecting data from Digital Nagriks. The aim of this bill is to provide rules for processing digital personal data that respect individuals' right to privacy, the need to handle personal data for necessary legal purposes, and any incidental uses. These accidental intents serve as the foundation for following Bill's guidelines.

The following guidelines are taken into consideration when framing the bill:

- The personal information of Nagriks that are used by different platforms and fiduciaries must be used in a way that is permitted by law.
- It should uphold the Nagrik connecter's fairness and openness.
- The purpose limitation principle states that information must be utilised for the intended purpose for which it was gathered.
- The data minimisation principle states that only the most important personal information should be gathered in order to achieve a certain goal.
- The principle of correctness of personal data stipulates that Nagarik's personal data must be kept up to date and that its accuracy must be guaranteed.

According to the storage restriction principle, Nagrik's personal information shouldn't be stored by default indefinitely. There should be no collection or processing of personal data that is prohibited by law, and it should be restricted to the time period required to carry out the particular purpose for which the data was gathered. In order to achieve this, reasonable precautions ought to be taken. The accountability principle states that whomever made the decision on the reason and the means of processing personal data should be held accountable.[24]

Different Aspect of the bill

Data gathered offline or online and then converted to digital form within India, as well as data processing conducted outside of India if it is related to Indian operations, are covered under the

[23] Dogra Ziya Siddiqui, Data Privacy Laws in India, 2 JUS CORPUS L.J. 538 (June-August 2022).
[24] Aditya Bashambu & Lavanya Chetwani, Critical Analysis: Digital Personal Data Protection Bill 2022, 3 JUS CORPUS L.J. 519 (December 2022).

 ISSN: 2582-6433

Digital Personal Data Protection Bill, 2022. Data over 100 years old, offline personal data, non-automated data, and personal purpose data are all excluded. The measure compels data fiduciaries to give data principals comprehensive, itemised disclosures in paper or electronic form, and it restricts data acquisition to legitimate reasons. With the ability to revoke consent at any moment, consent must be freely provided. Consent is considered given in some situations, such as emergencies, public order, or medical assistance. In addition to extra measures for processing children's data, the law lays out nine obligations for data fiduciaries and details the rights and responsibilities of data principals. With information on its composition, duties, and sanctions for noncompliance, it creates the Data Protection Board of India. In order to bring current laws into compliance with its requirements, the measure also modifies the Right to Information Act and the Information Technology Act of 2000.[25]

Major Flaws in the Digital Personal Data Protection Bill, 2022

- Sensitive personal information lacks strong protection in the 2022 bill because it merges personal and sensitive personal data categories which weakens protection for keys aspects of health and financial information.
- The bill includes "deemed consent" provisions that enable data collection without specific user agreements when public interests occur in connection with employment thus creating challenges regarding misuse and ambiguity regarding withdrawal options.
- The updated draft omits the data storage requirement in India because it allows companies to transfer information to unspecified "trusted geographies."
- The Data Protection Board faces problems because the Central Government has full control over it which creates doubts about unbiased data regulation.
- The bill fails to protect either offline or non-automated data therefore personal information within physical record systems remains at risk of improper use.
- The bill demands parental approval for child data handling creating obstacles for businesses operating in gaming and related industries because children must be eighteen years old to grant their consent. Harm definitions remain unclear in the bill making compliance difficult.
- The legislation grants extensive exceptions for government entities that enable them to withhold particular entities from data protection regulations through ambiguous terms

[25] Divyanshi Kaushal, The Digital Personal Data Protection Bill, 2022, 3 JUS CORPUS L.J. 747 (December 2022).

 ISSN: 2582-6433

such as "public order" and "national security" despite the Puttaswamy judgment on privacy.

- Under Amendment to RTI Act the government can restrict the public release of personal details through RTI which may reduce both transparency and governmental accountability.
- The bill presents no specific time frames which would determine how long data should stay after consent expiration or when a purpose's completion occurs thereby creating confusion in compliance enforcement. Broad Definition of Public Interest is that it allows data processing without explicit consent, increasing the risk of abuse. Delegated Legislation runs too wild due to numerous provisions that authorize Executive authority which diminishes legislative control thus elevating potential government discretion.
- Significant Data Fiduciaries (SDFs) enable the government to make extensive designations of data governance entities because they possess broad regulatory powers yet their designation process shows potential bias and political manipulation.[26]

THE BENEFITS OF THE BILL

Certain beneficial aspects of the bill can be that it brings in the first legal framework to bring in more transparency related to the processing of the data and resolve the ambiguous ambit of privacy that has been the bone of contention for a long now. It also calls for data minimisation which essentially means that the data to be collected should be minimised. It also elaborates on the aspect of storage limitation meaning that the data should be stored for the period that is necessary for the stated purpose. The government has pointed out that the said bill will bring ease of doing business, look forward to the privacy of individuals and data protection as well as cater to the public interests. In addition to the said benefits, the clause to the personal data of the children can be well inferred that the government has been quite considerate towards the breach of data and the cybercrimes happening against children and how they become prey of evils that they are not aware of. Thus, the parent's consent and the idea to correct or erase the data have also been welcomed.[27]

[26] Aditya Bashambu & Lavanya Chetwani, Critical Analysis: Digital Personal Data Protection Bill 2022, 3 JUS CORPUS L.J. 519 (December 2022).
[27] Divyanshi Kaushal, The Digital Personal Data Protection Bill, 2022, 3 JUS CORPUS L.J. 747 (December 2022).

 ISSN: 2582-6433

A BRIEF HISTORY OF THE DATA PROTECTION

Justice K. S. Puttaswamy (Retd) v Union of India[28]: In the given case which was decided in the year 2017, a nine-judge bench of the supreme court held that Indian citizens have a fundamental right to privacy under Article 218.

B.N. Srikrishna Committee, 2017: The Government appointed a committee under the leadership of B.N. Srikrishna in 2017 to look into the aspects of data protection and the committee submitted its report in 2018 along with a draft data protection bill.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021: The rules direct social media platforms to exercise greater diligence about the content on their sites.[29]

Conclusion

In an era of rapid digital transformation, cybersecurity is an enduring challenge that requires an evolving and integrated response. The evolving landscape of cyber threats from ransomware and phishing to AI enabled cyberattacks demands constant refinement of legal frameworks, technical Défense and organizational policy. While international laws like GDPR and CCPA have formed solid enforcement precedents, India's policy-framework around cybersecurity, being led by IT Act, 2000, and Digital Personal Data Protection Bill, 2023, suffers mostly from enforcement gap, flexibility and international cooperation. At the very least, a solid information security initiative incorporates a combination of legal based provisions, advanced security technologies, and risk management. Cyber risk mitigation cannot ignore business cybersecurity policy, public-private partnerships, and even international approaches. Legal enforcement needs to be made stronger; the population needs to be made more aware, and cross-border protection mechanisms need to be developed as necessary steps to have a proper digital ecosystem. As cybercriminals themselves keep refining their strategy, India's cybersecurity laws would also have to remain dynamic so they can keep pace with emerging threats while protecting privacy and innovation. Organizations require financial support to detect threats with artificial intelligence before establishing standard cyber resilience measures to meet enhanced regulatory standards. India must develop strategic plans which combine legal

[28] Justice K S. Puttaswamy (Retd) v Union of India AIR (2017) SC 4161
[29] Divyanshi Kaushal, The Digital Personal Data Protection Bill, 2022, 3 JUS CORPUS L.J. 747 (December 2022).

 ISSN: 2582-6433

progress and technological changes to improve its cybersecurity strength for protecting digital spaces for both citizens and businesses and government entities. Lastly, the war against cyber threats is a never-ending process which needs to be pursued in cooperation among legal institutions, policymakers, technology creators, and practitioners in cybersecurity. A balanced framework of cybersecurity based on legal liability, technological innovation, and international cooperation needs to be established in order to construct a safe and robust cyberspace.