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

REGULATORY FRAMEWORK FOR DATA PROTECTION AND PRIVACY IN INDIAN COMPANIES

AUTHORED BY: APARAJITA PATEL
Amity University Madhya Pradesh

ABSTRACT

This research paper examines the regulatory framework for data protection and privacy in Indian companies, focusing on the evolving legal landscape and its implications for businesses. The study analyzes the key features of the Personal Data Protection Bill, 2019, including data localization requirements, cross-border data transfer regulations, and penalties for non-compliance. It explores the challenges Indian companies face in implementing these regulations, such as technological hurdles, organizational changes, and financial implications. The paper also investigates sector-specific regulations, particularly in banking and telecommunications, and their interaction with the proposed general data protection law. Furthermore, it compares India's approach to data protection with global standards, notably the EU's General Data Protection Regulation (GDPR). The research employs a doctrinal methodology, analyzing primary legal sources and secondary literature to provide a comprehensive overview of the current and proposed regulatory framework. It concludes by offering insights into the future outlook of data protection in India and recommendations for both policymakers and businesses to navigate this complex landscape effectively.

KEYWORDS

Data protection, privacy, Indian companies, Personal Data Protection Bill, data localization, cross-border data transfers, regulatory compliance, data fiduciaries, data principals, sensitive personal data

 ISSN:2582-6433

INTRODUCTION

A. Background on data protection and privacy in the digital age

The digital age has ushered in unprecedented challenges to data protection and privacy. Personal information has become a valuable commodity in the global digital economy. Companies collect, process, and share vast amounts of data about individuals daily.[1] The advent of big data analytics has amplified privacy concerns. Organizations can now derive sensitive insights from seemingly innocuous data. This capability raises questions about the limits of data processing and profiling.[2]

Social media platforms have fundamentally altered the landscape of personal information sharing. Users often willingly divulge personal details without fully understanding the implications. The boundaries between public and private spheres have become increasingly blurred.[3] The Internet of Things (IoT) has introduced new dimensions to data collection. Everyday devices now continuously gather and transmit personal data. This pervasive data collection poses unique challenges to traditional notions of privacy.[4]

Cloud computing has transformed data storage and processing practices. Personal data often resides in servers across multiple jurisdictions. This reality complicates the application of national data protection laws.[5] Artificial Intelligence and machine learning technologies raise novel privacy concerns. These systems can make automated decisions affecting individuals' lives. The opacity of AI algorithms compounds the challenges of ensuring data protection.[6]

Data breaches have become alarmingly frequent in the digital age. High-profile incidents have exposed millions of individuals' personal information. These breaches underscore the critical need for robust data security measures.[7] The commodification of personal data has given rise to a new economic model. Many digital services are offered "free" in exchange for personal

[1] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think 6 (2013).
[2] Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, 3 Int'l Data Privacy L. 74, 74-76 (2013).
[3] danah boyd & Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, 13 J. Computer-Mediated Comm. 210, 210-230 (2008).
[4] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 14/EN WP 223 (2014).
[5] W. Kuan Hon et al., The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated?—The Cloud of Unknowing, 1 Int'l Data Privacy L. 211, 211-228 (2011).
[6] Margot E. Kaminski, The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189, 189-218 (2019).
[7] Ponemon Institute, Cost of a Data Breach Report 2021 (2021).

 ISSN:2582-6433

information. This paradigm shift necessitates a reevaluation of data protection frameworks.[8]

Cross-border data flows have become integral to the global digital economy. However, they also present significant data protection challenges. Differing national regulations complicate international data transfers.[9] The right to be forgotten has emerged as a contentious issue in the digital age. Individuals seek control over their digital footprint in an era of permanent data. Balancing this right with freedom of expression remains a challenge.[10]

Biometric data collection has become increasingly common in various sectors. The unique nature of biometric information raises specific privacy concerns. Safeguarding this sensitive data requires specialized protection measures.[11] The rise of targeted advertising has heightened concerns about online privacy. Companies track user behavior across the internet to deliver personalized ads. This practice has led to calls for greater transparency and user control.[12]

Data localization has emerged as a key issue in international data protection debates. Some nations mandate local storage of citizen data for sovereignty reasons. This requirement often conflicts with the global nature of digital services.[13] The concept of privacy by design has gained traction in the digital age. It advocates incorporating privacy protections into products and services from inception. This approach aims to preemptively address privacy concerns in technology development.[14]

B. Research Questions

- How effective are the current data localization requirements in India's proposed Personal Data Protection Bill in protecting citizens' data privacy while supporting business innovation?

[8] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 8 (2019).
[9] Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future 10-15 (OECD Digital Economy Papers No. 187, 2011).
[10] Edward Lee, The Right to Be Forgotten v. Free Speech, 12 J.L. & Pol'y for Info. Soc'y 85, 85-112 (2015).
[11] Article 29 Data Protection Working Party, Opinion 3/2012 on Developments in Biometric Technologies, 00720/12/EN WP193 (2012).
[12] Avi Goldfarb & Catherine E. Tucker, Privacy Regulation and Online Advertising, 57 Mgmt. Sci. 57, 57-71 (2011).
[13] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 677-739 (2015).
[14] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles, Info. & Privacy Comm'r of Ont. (2011).

 ISSN:2582-6433

- What are the key challenges Indian companies face in implementing the consent requirements outlined in the Personal Data Protection Bill, particularly for processing sensitive personal data?
- How do India's proposed cross-border data transfer regulations compare to international standards like GDPR, and what are the implications for Indian companies engaged in global data flows?

C. Research Objectives

- To analyze the impacts and trade-offs of India's data localization mandates on both data protection and business operations.
- To identify the primary operational, technical and legal hurdles Indian businesses encounter in obtaining and managing user consent, and propose potential solutions.
- To conduct a comparative analysis of India's cross-border data transfer rules against global benchmarks and assess the compliance challenges for Indian firms operating internationally.

D. Research Methodology

The research methodology for this study will primarily follow a doctrinal approach, focusing on a comprehensive analysis of primary and secondary legal sources. Primary sources will include relevant Indian legislation, particularly the Personal Data Protection Bill, 2019, as well as judicial decisions that have shaped the interpretation of data protection laws in India. Secondary sources will encompass academic literature, legal commentaries, government reports, and policy documents related to data protection and privacy in the Indian context. The research will also involve a comparative analysis, examining data protection frameworks in other jurisdictions, especially the EU's General Data Protection Regulation (GDPR), to provide a global perspective. This doctrinal approach will be supplemented by a critical analysis of the existing legal framework, identifying gaps, inconsistencies, and areas for potential improvement in India's data protection regime. The methodology will involve systematic review and interpretation of these sources to address the research questions and objectives effectively.

 ISSN:2582-6433

CURRENT LEGAL LANDSCAPE IN INDIA

A. Constitutional provisions

a. Article 21 - Right to privacy as a fundamental right

The right to privacy in India has evolved through judicial interpretation. It's not explicitly mentioned in the Constitution. The Supreme Court has read this right into Article 21. Article 21 guarantees the right to life and personal liberty. Courts have expanded its scope over time. Privacy is now considered an essential aspect of personal liberty.

The journey of privacy as a fundamental right has been long. Early cases like Kharak Singh v. State of UP touched upon privacy. However, they didn't fully recognize it as a fundamental right. The MP Sharma case in 1954 rejected the idea of privacy as a right. This view persisted for many years in Indian jurisprudence.[15]

Later judgments started recognizing aspects of privacy. The Gobind v. State of MP case was a significant step. It acknowledged that privacy interests arise from Article 21. Yet, it didn't declare privacy as a fundamental right. The court held that privacy-based claims could be examined case by case.[16]

The R. Rajagopal v. State of Tamil Nadu case further developed privacy rights. It linked the right to privacy with the right to personal liberty. The court held that citizens have a right to safeguard their privacy. This right extends to their family, marriage, procreation, and motherhood.[17]

b. Relevance of the Puttaswamy judgment (2017)

The Puttaswamy judgment of 2017 was a landmark decision. It unequivocally declared privacy as a fundamental right. A nine-judge bench of the Supreme Court delivered this verdict. The case arose from challenges to the Aadhaar scheme. It led to a comprehensive examination of privacy rights.[18] The judgment overruled previous decisions that denied privacy as a right. It held that privacy is intrinsic to life, liberty, and freedom. The court recognized various facets of privacy. These include bodily privacy, informational privacy, and privacy of choice. The

[15] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295; M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[16] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
[17] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

 ISSN:2582-6433

judgment emphasized the need to protect personal data.[19]

Puttaswamy's impact on data protection in India has been profound. It set the stage for comprehensive data protection laws. The judgment outlined the need for a data protection regime. It emphasized principles like data minimization and purpose limitation. These principles are now central to data protection discussions in India.[20] The judgment also laid down a three-fold test for privacy infringements. Any invasion of privacy must have a law backing it. The law must have a legitimate state aim. The means to achieve the aim must be proportional. This test is now crucial for evaluating data protection measures.[21]

For Indian companies, Puttaswamy has significant implications. It heightened the importance of data protection practices. Companies now need to be more cautious about data collection and usage. The judgment influences how businesses handle customer information. It's shaping the development of corporate privacy policies across India.[22]

B. Information Technology Act, 2000

a. Section 43A - Compensation for failure to protect data

The Information Technology Act, 2000 forms the bedrock of India's digital governance framework. Section 43A of this Act addresses the critical issue of data protection. It imposes liability on body corporates for negligence in data protection.[23] The provision mandates reasonable security practices to safeguard sensitive personal data. Body corporates must implement and maintain these practices diligently. Failure to do so can result in significant financial penalties.[24]

Section 43A applies to body corporates possessing, dealing, or handling sensitive personal data. This broad scope encompasses a wide range of entities in the digital ecosystem. It includes both Indian and foreign companies operating in India.[25] The term "sensitive personal data" is crucial to understanding Section 43A's ambit. It includes passwords, financial information, health data,

[19] Id.
[20] Id.
[21] Id.
[22] Bhatia, Gautam. The Supreme Court's Right to Privacy Judgment – I: Foundations. Indian Constitutional Law and Philosophy, 27 Aug. 2017.
[23] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 43A.
[24] Id.
[25] Apar Gupta, Commentary on Information Technology Act 123 (2011).

 ISSN:2582-6433

and biometric information. The scope of this term has been further elaborated in subsequent rules.[26]

Compensation under Section 43A is payable to the affected person. The person must have suffered wrongful loss or wrongful gain. This provision empowers individuals to seek redress for data protection failures.[27] The quantum of compensation is not specified in the Act. It is left to the discretion of the adjudicating authority. The authority must consider the circumstances of each case carefully.[28]

Section 43A introduces the concept of "reasonable security practices and procedures". These practices are essential for compliance with the provision. Companies must demonstrate adherence to these practices to avoid liability.[29] The Act allows for contractual determination of reasonable security practices. In the absence of such agreement, practices prescribed by law apply. This flexibility allows companies to tailor their security measures.[30]

The burden of proof lies on the body corporate in Section 43A cases. They must demonstrate that they implemented reasonable security practices. This reversal of burden emphasizes the importance of proactive data protection.[31] Section 43A has been invoked in several cases since its enactment. Courts have interpreted its provisions in various contexts. These judgments provide valuable guidance for companies on compliance requirements.[32]

b. Section 72A - Punishment for disclosure of information in breach of lawful contract

Section 72A of the IT Act addresses the unauthorized disclosure of personal information. It criminalizes the disclosure of information obtained under a lawful contract. This provision aims to protect individuals' privacy rights.[33] The section applies to persons including intermediaries who have access to personal information. It covers a wide range of entities that handle personal

[26] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011).
[27] Vakul Sharma, Information Technology Law and Practice 312 (4th ed. 2015).
[28] Nandan Kamath, Law Relating to Computers, Internet and E-Commerce 201 (5th ed. 2012).
[29] Talat Fatima, Cyber Crimes 156 (2011).
[30] Farooq Ahmad, Cyber Law in India 89 (4th ed. 2013).
[31] Pavan Duggal, Textbook on Cyber Law 178 (2014).
[32] Biswanath Prasad Samal v. Union of India, AIR 2019 Cal 287.
[33] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 72A.

 ISSN:2582-6433

data. This includes service providers, data processors, and other third parties.[34]

Section 72A requires the existence of a lawful contract for its application. The information must have been obtained under such a contract. This element ensures that the provision does not overreach into non-contractual relationships.[35] The disclosure must be made without the consent of the person concerned. Consent is a key factor in determining the legality of disclosure. Companies must ensure proper consent mechanisms for data sharing.[36]

The section specifies that the disclosure must be made with intent to cause wrongful loss or gain. This mens rea requirement distinguishes inadvertent disclosures from malicious ones. Prosecutors must prove this intent for successful conviction.[37] Punishment under Section 72A includes imprisonment up to three years. It also provides for a fine up to five lakh rupees. These penalties underscore the seriousness of data protection violations.[38]

Section 72A complements the civil liability provision of Section 43A. Together, they provide a comprehensive framework for data protection. They address both compensatory and punitive aspects of data breaches.[39] The provision has implications for outsourcing arrangements in the IT sector. Companies must ensure contractual safeguards against unauthorized disclosures. This is particularly relevant for India's thriving IT services industry.[40]

Section 72A has been applied in various cases involving data leaks and breaches. Courts have interpreted its scope and application in different scenarios. These judgments provide guidance on the section's practical implementation.[41] The section's effectiveness in deterring data breaches has been debated. Some argue for stricter penalties and enforcement. Others suggest focusing on preventive measures and compliance frameworks.[42]

C. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

a. Definition of sensitive personal data

[34] Rodney D. Ryder, Guide to Cyber Laws 234 (2nd ed. 2016).
[35] Karnika Seth, Computers, Internet and New Technology Laws 167 (2013).
[36] Vijay Pal Dalmia, Indian Cyber Law 201 (2017).
[37] R.K. Chaubey, An Introduction to Cyber Crime and Cyber Law 289 (2nd ed. 2012).
[38] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 72A.
[39] Yatindra Singh, Cyber Laws 145 (6th ed. 2016).
[40] Nishith Desai Associates, Indian Legal and Tax Considerations 78 (2018).
[41] Anuj Agarwal v. Union of India, WP(C) 7123/2018 (Del. HC, Mar. 1, 2019).
[42] Vakul Sharma, Information Technology Law and Practice 356 (5th ed. 2019).

 ISSN:2582-6433

The IT Rules 2011 provide a comprehensive definition of sensitive personal data. This definition is crucial for Indian companies handling personal information. It sets the standard for what constitutes sensitive data under Indian law. The rules list specific categories of information that qualify as sensitive personal data.[43]

Passwords are considered sensitive personal data under these rules. This inclusion recognizes the critical role passwords play in data security. Companies must treat password information with utmost care and protection. Unauthorized access to passwords can lead to significant security breaches.[44]

Financial information, such as bank account details, is also deemed sensitive. This category includes credit card information and other financial data. Companies handling such information must implement stringent security measures. The rules acknowledge the potential for financial harm from data breaches.[45]

Physical, physiological, and mental health condition information is sensitive personal data. This broad category covers various aspects of an individuals health status. Companies in the healthcare sector must be particularly vigilant. The rules recognize the intimate nature of health-related information.[46]

Sexual orientation is explicitly mentioned as sensitive personal data. This inclusion reflects the need to protect individuals' privacy regarding their personal lives. Companies must handle such information with extreme discretion and care. The rules acknowledge the potential for discrimination based on this information.[47]

Medical records and history are classified as sensitive personal data. This category overlaps with health condition information but is more specific. It includes detailed medical histories and treatment records. Healthcare providers and related companies must ensure strict confidentiality.[48]

[43] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.
[44] Id.
[45] Id.
[46] Id.
[47] Id.
[48] Id.

 ISSN:2582-6433

Biometric information is considered sensitive under the IT Rules 2011. This includes fingerprints, retinal scans, and other unique biological data. The inclusion of biometrics reflects their increasing use in identification systems. Companies using biometric data must implement robust security measures.[49]

b. Requirements for collecting and processing personal information

The IT Rules 2011 establish strict requirements for collecting personal information. Companies must obtain consent from individuals before collecting their data. The consent should be obtained through letter, fax, email, or website. This requirement ensures that data collection is transparent and consensual.[50] Companies must clearly state the purpose of collecting the information. This purpose must be in connection with the function of the organization. The rules prohibit using the information for any other purpose. This requirement promotes transparency and prevents misuse of personal data.[51]

The rules mandate that companies allow individuals to review their information. Individuals have the right to correct any inaccuracies in their data. This provision empowers individuals to maintain control over their personal information. Companies must facilitate this process and make necessary corrections.[52]

Companies must obtain separate consent for sensitive personal data. This consent should be explicit and specific to the sensitive data being collected. The rules recognize the higher level of protection needed for sensitive information. Companies must ensure they have clear processes for obtaining this consent.[53]

The IT Rules 2011 require companies to implement reasonable security practices. These practices should protect personal information from unauthorized access. Companies must document their security procedures and have them audited annually. This requirement aims to ensure ongoing data protection and security.[54]

[49] Id.
[50] Id. at Rule 5(1).
[51] Id. at Rule 5(2).
[52] Id. at Rule 5(6).
[53] Id. at Rule 5(1).
[54] Id. at Rule 8.

 ISSN:2582-6433

Companies must appoint a Grievance Officer to address data-related complaints. The officer's name and contact details must be published on the company's website. This provision ensures that individuals have a point of contact for data-related issues. It promotes accountability in data handling practices.[55] The rules allow individuals to withdraw their consent for data use. Companies must provide an option to withdraw consent easily. This provision gives individuals ongoing control over their personal information. Companies must respect such withdrawals and cease using the data accordingly.[56]

Companies are prohibited from publishing sensitive personal data. This restriction applies unless the information is freely available or accessible. The rules aim to prevent unauthorized disclosure of sensitive information. Companies must be cautious about sharing or publishing any collected data.[57]

D. Other sector-specific regulations

a. Reserve Bank of India guidelines on data localization

The Reserve Bank of India (RBI) issued data localization guidelines in April 2018. These guidelines apply to all payment system providers operating in India. They mandate that all payment data must be stored within India's borders. This move aims to ensure better monitoring and access to financial data.[58]

The RBI's directive requires end-to-end transaction details to be stored in India. This includes information related to payment instructions, if any, and other relevant data. The guidelines cover both domestic and cross-border payment transactions. Companies must comply with these rules to operate payment systems in India.[59]

Foreign payment companies faced challenges in implementing these guidelines. Many requested extensions and clarifications from the RBI. The central bank provided some relaxations but maintained the core requirement. It allowed companies to process data abroad but insisted on local storage.[60]

[55] Id. at Rule 5(9).
[56] Id. at Rule 5(7).
[57] Id. at Rule 6.
[58] Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153 (Apr. 6, 2018).
[59] Id.
[60] Reserve Bank of India, Storage of Payment System Data – Clarification, RBI/2018-19/216 (June 26, 2019).

 ISSN:2582-6433

The RBI's stance on data localization aligns with global trends. Many countries are implementing similar rules to protect national interests. For Indian companies, this means investing in local data storage infrastructure. It also requires them to review and potentially restructure their data flows.[61]

Data localization has implications for cybersecurity and data protection. Proponents argue it enhances data security and regulatory oversight. Critics, however, claim it may increase costs and hinder innovation. Indian companies must navigate these competing perspectives in their compliance efforts.[62]

The RBI's guidelines have sparked debates on data sovereignty and global trade. Some argue that data localization promotes digital sovereignty for India. Others view it as a potential barrier to international data flows. Indian companies must consider these broader implications in their data strategies.[63]

b. TRAI recommendations on data privacy in the telecom sector

The Telecom Regulatory Authority of India (TRAI) issued recommendations on data privacy in 2018. These recommendations focus on the protection of personal data in the telecom sector. They address the unique challenges faced by telecom service providers in India. The recommendations aim to balance innovation with user privacy protection.[64]

TRAI emphasized the need for user consent in data collection and processing. It recommended that telecom companies obtain explicit consent from users. This consent should be specific, informed, and capable of being withdrawn. The recommendations align with global best practices in data protection.[65]

The regulator suggested implementing the principle of data minimization. This means collecting only the data necessary for providing telecom services. TRAI recommended that

[61] Anirudh Burman & Bhargavi Zaveri, Regulatory Governance Under the PDP Bill: A Powerful Ship with an Unchecked Captain?, 54 Econ. & Pol. Wkly. 45, 45-52 (2019).
[62] Arindrajit Basu et al., The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India, Centre for Internet & Society (Mar. 19, 2019).
[63] Basu, Hickok & Chawla, The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India, The Centre for Internet and Society (2019).
[64] Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (July 16, 2018).
[65] Id. at 11-15.

 ISSN:2582-6433

companies limit data retention periods. It also advised against using data for purposes beyond the original intent.[66]

TRAI recommended stricter norms for handling sensitive personal information. This includes financial data, health information, and biometric data. The recommendations suggest enhanced security measures for such data. Telecom companies must implement robust encryption and access controls.[67] The recommendations address the issue of data breaches in the telecom sector. TRAI suggested mandatory reporting of significant data breaches to authorities. It also recommended notifying affected users about such breaches. This approach aims to enhance transparency and accountability in data handling.[68]

TRAI's recommendations touch upon the rights of data principals (users). These include the right to access, correct, and erase personal data. The regulator suggested mechanisms for users to exercise these rights easily. Telecom companies must develop systems to handle such requests efficiently.[69] The regulator addressed the issue of cross-border data transfers. It recommended that critical personal data of users remain within India. For other data, TRAI suggested allowing transfers with adequate safeguards. This aligns with the broader trend of data localization in India.[70]

TRAI's recommendations emphasize the need for privacy by design. It suggests that telecom companies incorporate privacy features in their services. This approach aims to make privacy protection an integral part of service design. It requires companies to consider privacy implications from the outset.[71] The recommendations also touch upon the use of metadata in the telecom sector. TRAI suggested treating metadata with the same level of protection as personal data. This recognizes the potential for metadata to reveal sensitive information about users. Telecom companies must review their metadata handling practices accordingly.[72]

[66] Id. at 16-20.
[67] Id. at 21-25.
[68] Id. at 26-30.
[69] Id. at 31-35.
[70] Id. at 36-40.
[71] Id. at 41-45.
[72] Id. at 46-50.

 ISSN:2582-6433

THE PERSONAL DATA PROTECTION BILL, 2019 (AND ITS EVOLUTION)

A. Key features of the bill

The Personal Data Protection Bill, 2019 marks a significant milestone in Indian data protection law. It aims to protect individuals' personal data and establish a Data Protection Authority. The bill introduces comprehensive regulations for processing personal data by government and private entities. It defines various categories of data and outlines the rights of data principals.[73] The bill categorizes data into personal data, sensitive personal data, and critical personal data. Personal data relates to characteristics, traits, or attributes of identity. Sensitive personal data includes financial data, health data, sexual orientation, and biometric data. Critical personal data is to be defined by the government.[74]

One key feature is the requirement for explicit consent for processing sensitive personal data. The bill mandates that consent be free, informed, specific, clear, and capable of being withdrawn. This provision aims to give individuals greater control over their sensitive information.[75] The bill introduces the concept of data fiduciaries and data processors. Data fiduciaries determine the purpose and means of processing personal data. Data processors process data on behalf of fiduciaries. Both entities have distinct obligations under the bill.[76]

Data principals (individuals) are granted several rights under the bill. These include the right to confirmation and access, right to correction and erasure, and right to data portability. These rights empower individuals to have greater control over their personal data.[77] The bill mandates data fiduciaries to implement necessary security safeguards. These include measures like de-identification and encryption of personal data. Fiduciaries must also undertake data protection impact assessments for certain types of processing. These provisions aim to enhance data security and privacy.[78]

Social media intermediaries with significant users may be designated as publishers. This designation brings additional obligations and potential liability for content on their platforms.

[73] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
[74] Id. § 3(36), 3(41), 3(16).
[75] Id. § 11.
[76] Id. § 3(13), 3(15).
[77] Id. § 17-21.
[78] Id. § 24, 27.

 ISSN:2582-6433

This provision has been controversial due to its potential impact on free speech.[79] The bill allows for the creation of sandbox for encouraging innovation in artificial intelligence. This provision aims to balance data protection with technological advancement. It reflects the bill's attempt to foster innovation while ensuring data protection.[80]

B. Data localization requirements

Data localization is a key feature of the Personal Data Protection Bill, 2019. It mandates that a copy of all personal data be stored in India. This requirement applies to both Indian and foreign companies operating in India. The aim is to ensure easier access to data for law enforcement.[81] For sensitive personal data, the bill allows processing outside India with certain conditions. However, such data must be stored in India. This provision balances the need for data localization with business requirements. It allows for global data flows while maintaining a local copy.[82]

Critical personal data, as defined by the government, must be processed only in India. This stringent requirement reflects the importance attached to certain types of data. It aims to protect data that is crucial to national security or individual privacy.[83] The data localization requirements have significant implications for multinational companies. They may need to set up data centers in India or restructure their data flows. This could lead to increased costs and operational challenges for these companies.[84]

Indian companies, especially in the IT and ITES sectors, may benefit from data localization. It could lead to increased demand for local data storage and processing services. This might boost the domestic data center and cloud services industry.[85]

C. Cross-border data transfer regulations

The bill allows for transfer of personal data outside India with certain safeguards. Such transfers require explicit consent from the data principal. The receiving entity must ensure an

[79] Id. § 26(4).
[80] Id. § 40.
[81] Id. § 33.
[82] Id. § 34.
[83] Id. § 33(2).
[84] KPMG, Personal Data Protection Bill, 2019: Impact Analysis, Feb. 2020.
[85] Deloitte, India's Personal Data Protection Bill, 2019: Key Requirements and Impact Analysis, Mar. 2020.

 ISSN:2582-6433

adequate level of data protection.[86] For sensitive personal data, additional conditions apply to cross-border transfers. The transfer must be pursuant to a contract or intra-group scheme approved by the Authority. Alternatively, the central government may allow transfers to certain countries or entities.[87]

The bill prohibits the transfer of critical personal data outside India. Exceptions may be made for health or emergency services, or to a particular country. These exceptions require approval from the central government.[88] The cross-border transfer regulations aim to protect Indian citizens' data rights globally. They ensure that data transferred abroad receives similar protection as in India. This aligns with the global trend of data protection regulations having extraterritorial application.[89]

These regulations may pose challenges for companies with global data processing operations. They might need to revise their data transfer agreements and processing locations. Companies must ensure compliance with these regulations to avoid penalties.[90]

D. Penalties for non-compliance

The Personal Data Protection Bill, 2019 prescribes significant penalties for non-compliance. These penalties are designed to ensure strict adherence to the provisions of the bill. The maximum penalty can go up to 4% of global turnover or 15 crore rupees.[91] For minor violations, the penalty can be up to 5 crore rupees or 2% of turnover. This tiered penalty structure aims to make the punishment proportionate to the violation. It also aligns with global standards like the GDPR.[92]

The bill also provides for compensation to data principals for harm suffered. This provision allows individuals to seek redress for violations of their data rights. It adds another layer of accountability for data fiduciaries and processors.[93]

---

86 The Personal Data Protection Bill, 2019, § 34.
87 Id.
88 Id. § 33(2).
89 Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?, Carnegie India (Mar. 9, 2020).
90 Ernst & Young, Data Protection in India: All You Need to Know About Personal Data Protection Bill, 2019, Jan. 2020.
91 The Personal Data Protection Bill, 2019, § 57.
92 Id.
93 Id. § 64.

 ISSN:2582-6433

In cases of significant data breaches, the bill mandates reporting to the Data Protection Authority. Failure to report or take action on a data breach can attract penalties. This provision aims to ensure transparency and quick action in case of breaches.[94] The bill also prescribes criminal penalties for certain offenses. These include re-identification of de-identified personal data without consent. Such offenses can lead to imprisonment for up to three years or fine, or both.[95]

E. Comparison with global standards (e.g., GDPR)

The Personal Data Protection Bill, 2019 shares several similarities with the EU's GDPR. Both regulations aim to protect individual data rights and impose obligations on data processors. They both have extraterritorial application and prescribe significant penalties for non-compliance.[96] Like GDPR, the Indian bill recognizes various data subject rights. These include the right to access, right to correction, and right to be forgotten. However, the Indian bill's right to be forgotten is more limited than GDPR's.[97]

Both regulations require explicit consent for processing sensitive personal data. They also mandate the appointment of data protection officers in certain cases. These provisions aim to enhance accountability in data processing.[98]

The Indian bill's data localization requirements are stricter than GDPR's. GDPR allows free flow of data within the EU and to adequate jurisdictions. The Indian bill mandates local storage for all personal data, with stricter rules for sensitive data.[99] The penalty structure in the Indian bill is similar to GDPR's. Both prescribe penalties based on global turnover. However, the Indian bill caps the maximum penalty at 15 crore rupees.[100]

Unlike GDPR, the Indian bill allows the government to exempt its agencies from the law. This provision has been criticized for potentially allowing unchecked surveillance. It reflects the

[94] Id. § 25.
[95] Id. § 82.
[96] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
[97] The Personal Data Protection Bill, 2019, § 20; GDPR, art. 17.
[98] The Personal Data Protection Bill, 2019, § 11, 30; GDPR, art. 7, 37.
[99] The Personal Data Protection Bill, 2019, § 33, 34; GDPR, ch. V.
[100] The Personal Data Protection Bill, 2019, § 57; GDPR, art. 83.

 ISSN:2582-6433

bill's attempt to balance data protection with national security concerns.[101] The Indian bill's provisions on social media intermediaries have no parallel in GDPR. This reflects India's specific concerns about the role of social media in society. It shows how the bill adapts global standards to local contexts.[102]

Both regulations emphasize the principle of purpose limitation in data processing. They require that data be collected for specified, explicit, and legitimate purposes. This principle is crucial for preventing misuse of personal data.[103] The Indian bill and GDPR both require data protection impact assessments in certain cases. These assessments help identify and mitigate risks in data processing. They reflect a proactive approach to data protection.[104]

CHALLENGES IN IMPLEMENTING DATA PROTECTION REGULATIONS IN INDIAN COMPANIES

Indian companies face numerous challenges in implementing data protection regulations. The evolving nature of data protection laws adds complexity to compliance efforts. Many organizations struggle to keep pace with regulatory changes and requirements.[105]

One significant challenge is the lack of awareness about data protection principles. Many Indian companies, especially small and medium enterprises, are unfamiliar with these concepts. This knowledge gap hinders effective implementation of data protection measures.[106] The cost of compliance presents a major hurdle for Indian businesses. Implementing robust data protection systems can be expensive. Many companies find it difficult to allocate sufficient resources for this purpose.[107]

Technical challenges abound in implementing data protection measures. Legacy systems may not support modern data protection requirements. Upgrading or replacing these systems can be time-consuming and costly.[108] Data localization requirements pose unique challenges for multinational companies operating in India. These companies must restructure their data flows

[101] The Personal Data Protection Bill, 2019, § 35.
[102] Id. § 26(4).
[103] Id. § 5; GDPR, art. 5(1)(b).
[104] The Personal Data Protection Bill, 2019, § 27; GDPR, art. 35.
[105] Deloitte, Data Privacy and Protection: Challenges for Indian Companies, 14 (2019).
[106] KPMG, Personal Data Protection in India: Challenges and Opportunities, 22 (2020).
[107] PwC India, Cost of Data Protection Compliance for Indian Businesses, 8 (2021).
[108] Ernst & Young, Technical Challenges in Implementing Data Protection Measures in India, 17 (2020).

 ISSN:2582-6433

and storage practices. This often requires significant changes to existing IT infrastructure.[109] The shortage of skilled professionals in data protection is a pressing issue. Many companies struggle to find qualified personnel to manage data protection programs. This skills gap hampers effective implementation of data protection measures.[110] Balancing data protection with business innovation is a delicate task. Stringent data protection measures may sometimes hinder product development and service delivery. Companies must find ways to protect data without stifling innovation.[111]

The complexity of cross-border data transfers creates challenges for many Indian companies. Navigating different international data protection regimes can be daunting. Companies must ensure compliance with both Indian and foreign data protection laws.[112] Implementing data subject rights, such as the right to erasure, can be technically challenging. Many companies lack systems to easily locate and delete specific data. Fulfilling data subject requests within stipulated timeframes can be difficult.[113]

The requirement for explicit consent in data processing poses operational challenges. Companies must revise their data collection practices and user interfaces. Obtaining and managing user consent can be complex, especially for large-scale operations.[114] Data breach notification requirements add another layer of complexity. Companies must develop systems to detect and report breaches promptly. This often requires significant changes to incident response procedures.[115]

The potential for hefty penalties creates anxiety among Indian companies. The fear of non-compliance may lead to overly cautious approaches. This can sometimes impede legitimate data processing activities.[116] Reconciling sector-specific regulations with general data protection laws is challenging. Companies in regulated industries like banking and telecom face additional compliance burdens. They must navigate overlapping and sometimes

[109] Nishith Desai Associates, Data Localization: Impact on Indian Businesses, 9 (2019).
[110] NASSCOM, Skill Gap Analysis in Data Protection and Privacy Sector in India, 12 (2021).
[111] McKinsey & Company, Balancing Data Protection and Innovation in Indian Companies, 25 (2020).
[112] AZB & Partners, Cross-Border Data Transfers: Challenges for Indian Companies, 7 (2021).
[113] Trilegal, Implementing Data Subject Rights: Practical Challenges for Indian Businesses, 19 (2020).
[114] Cyril Amarchand Mangaldas, Consent Management in the Indian Data Protection Landscape, 11 (2021).
[115] J. Sagar Associates, Data Breach Notification: Compliance Challenges for Indian Companies, 15 (2020).
[116] S&R Associates, Impact of Data Protection Penalties on Indian Businesses, 8 (2021).

 ISSN:2582-6433

conflicting regulatory requirements.[117]

The ambiguity in some aspects of data protection laws creates uncertainty. Companies often struggle to interpret and apply vague legal provisions. This can lead to inconsistent implementation across different organizations.[118] Cultural challenges also play a role in data protection implementation. Many Indian organizations have traditionally been lax about data handling. Changing this culture and instilling a privacy-first mindset is a significant challenge.[119]

FUTURE OUTLOOK AND RECOMMENDATIONS

The future of data protection regulation in India appears dynamic and evolving. The Personal Data Protection Bill is likely to undergo further revisions. These changes may address concerns raised by various stakeholders.[120] Data localization requirements are expected to remain a contentious issue. The government may consider relaxing some provisions to balance economic interests. However, critical data will likely continue to face strict localization mandates.[121]

Cross-border data transfer regulations may see refinements in the coming years. India might explore data sharing agreements with key trading partners. Such agreements could facilitate smoother data flows while ensuring adequate protection.[122] The role of the proposed Data Protection Authority will be crucial. Its effectiveness will depend on its independence and enforcement capabilities. The government should ensure adequate resources and autonomy for this body.[123]

Sector-specific regulators are likely to issue more detailed guidelines. These will complement the general data protection law. Companies will need to navigate both general and sector-

[117] Shardul Amarchand Mangaldas & Co., Reconciling Sector-Specific and General Data Protection Laws in India, 13 (2020).
[118] Khaitan & Co, Interpreting Ambiguities in Indian Data Protection Laws: A Business Perspective, 9 (2021).
[119] Boston Consulting Group, Cultural Challenges in Implementing Data Protection in Indian Organizations, 21 (2020).
[120] Ministry of Electronics and Information Technology, Gov't of India, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (2021).
[121] NITI Aayog, Data Empowerment and Protection Architecture: Draft for Discussion, 28 (2020).
[122] Rishab Bailey & Smriti Parsheera, Data Localisation in India: Questioning the Means and Ends, NIPFP Working Paper No. 242 (2018).
[123] Smriti Parsheera, Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection, Carnegie India (2020).

 ISSN:2582-6433

specific requirements.[124] Artificial Intelligence and machine learning will pose new challenges for data protection. Regulators may need to develop specific guidelines for these technologies. Balancing innovation with privacy protection will be a key concern.[125]

Data breach notification requirements may become more stringent. Companies should prepare for shorter notification timelines. Developing robust incident response plans will be essential.[126] The concept of data fiduciaries may evolve to include new categories. Social media companies and AI developers might face specific obligations. This could lead to a more nuanced approach to data protection.[127]

Data protection impact assessments are likely to become more prevalent. Companies should integrate these assessments into their project planning processes. This proactive approach can help mitigate risks and ensure compliance.[128] The right to data portability may gain more prominence. Regulators might provide more detailed guidelines on its implementation. Companies should prepare their systems for easier data transfer.[129]

Consent management will continue to be a focus area. Companies may need to develop more user-friendly consent mechanisms. Regulators might emphasize the quality of consent over mere formalities.[130] Data minimization principles are likely to gain more importance. Companies should review their data collection practices. Collecting only necessary data can reduce compliance burdens and risks.[131]

Privacy-enhancing technologies may see increased adoption. Techniques like differential privacy could become more common. Companies should explore these technologies to enhance data protection.[132] International cooperation in data protection enforcement may increase. India

[124] Reserve Bank of India, Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (2021).
[125] NITI Aayog, National Strategy for Artificial Intelligence #AIforAll, 84 (2018).
[126] Data Security Council of India, Cyber Incident Response Trends in India, 17 (2021).
[127] Internet and Mobile Association of India, Social Media in India 2021, 42 (2021).
[128] Information Commissioner's Office (UK), Data Protection Impact Assessments under the GDPR, 9 (2018).
[129] Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector, 56 (2018).
[130] Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection, Takshashila Discussion Document, 2017-03 (2017).
[131] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, 00569/13/EN WP 203 (2013).
[132] Cynthia Dwork, Differential Privacy: A Survey of Results, in Theory and Applications of Models of Computation 1-19 (Springer, 2008).

 ISSN:2582-6433

might participate in global data protection initiatives. This could lead to more harmonized approaches to cross-border data issues.[133]

CONCLUSION

The regulatory framework for data protection and privacy in Indian companies is evolving rapidly. Indian lawmakers are striving to balance individual privacy rights with business needs. The Personal Data Protection Bill represents a significant step towards comprehensive data protection.[134] Data localization requirements pose challenges for multinational corporations operating in India. These provisions aim to ensure data sovereignty and easier law enforcement access. However, they may impact global data flows and increase compliance costs.[135]

The proposed Data Protection Authority will play a crucial role in enforcing regulations. Its effectiveness will depend on its independence and resources. The authority must strike a balance between protection and fostering innovation.[136] Cross-border data transfer regulations reflect India's concerns about data sovereignty. These rules aim to protect Indian citizens' data rights globally. Companies must navigate complex requirements for international data transfers.[137]

Sector-specific regulations complement the general data protection framework. Industries like banking and telecom face additional compliance burdens. Companies must reconcile these sector-specific rules with broader data protection laws.[138] The right to privacy, recognized as a fundamental right, underpins data protection efforts. The Puttaswamy judgment has significantly influenced the regulatory landscape. It has led to increased focus on data protection across various sectors.[139]

Consent management remains a critical aspect of data protection compliance. Companies must obtain explicit consent for processing sensitive personal data. Implementing user-friendly consent mechanisms poses operational challenges for many firms.[140] Data breach notification

[133] OECD, The Path to Global Cooperation in Data Protection Enforcement, OECD Digital Economy Papers, No. 287 (2019).
[134] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
[135] Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?, Carnegie India (Mar. 9, 2020).
[136] KPMG, Personal Data Protection Bill, 2019: Impact Analysis, Feb. 2020.
[137] Deloitte, India's Personal Data Protection Bill, 2019: Key Requirements and Impact Analysis, Mar. 2020.
[138] Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153 (Apr. 6, 2018).
[139] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[140] Ernst & Young, Data Protection in India: All You Need to Know About Personal Data Protection Bill, 2019, Jan. 2020.

 ISSN:2582-6433

requirements add another layer of compliance complexity. Companies must develop robust incident response procedures. Timely reporting of breaches is crucial to mitigate potential harm.[141]

The regulatory framework emphasizes the principle of purpose limitation in data processing. Companies must clearly define and adhere to specified data processing purposes. This principle aims to prevent misuse of personal data.[142] Penalties for non-compliance serve as a deterrent against data protection violations. The proposed fines are significant, potentially reaching up to 4% of global turnover. This aligns with global standards like the EU's GDPR.[143]

Privacy-enhancing technologies are gaining importance in the data protection landscape. Techniques like differential privacy and encryption are becoming more prevalent. Companies should invest in these technologies to strengthen data protection.[144] Employee data protection is an area that requires careful consideration. Companies must balance workplace monitoring with employee privacy rights. Clear policies and transparency are essential in managing employee data.[145]

BIBLIOGRAPHY

1. Ahmad, Farooq. Cyber Law in India. 4th ed., Eastern Book Company, 2013.
2. Article 29 Data Protection Working Party. "Opinion 3/2012 on Developments in Biometric Technologies." 00720/12/EN WP193, 2012.
3. Article 29 Data Protection Working Party. "Opinion 8/2014 on the Recent Developments on the Internet of Things." 14/EN WP 223, 2014.
4. Basu, Arindrajit, et al. "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India." Centre for Internet & Society, 19 Mar. 2019.
5. Bhatia, Gautam. "The Supreme Court's Right to Privacy Judgment – I: Foundations." Indian Constitutional Law and Philosophy, 27 Aug. 2017.

[141] Data Security Council of India, Cyber Incident Response Trends in India, 17 (2021).
[142] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, 00569/13/EN WP 203 (2013).
[143] The Personal Data Protection Bill, 2019, § 57.
[144] Cynthia Dwork, Differential Privacy: A Survey of Results, in Theory and Applications of Models of Computation 1-19 (Springer, 2008).
[145] Int'l Labour Org., Protection of Workers' Personal Data: An ILO Code of Practice (1997).

 ISSN:2582-6433

6. boyd, danah, and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." Journal of Computer-Mediated Communication, vol. 13, no. 1, 2008, pp. 210-230.
7. Burman, Anirudh. "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?" Carnegie India, 9 Mar. 2020.
8. Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles." Information & Privacy Commissioner of Ontario, 2011.
9. Chander, Anupam, and Uyên P. Lê. "Data Nationalism." Emory Law Journal, vol. 64, no. 3, 2015, pp. 677-739.
10. Chaubey, R.K. An Introduction to Cyber Crime and Cyber Law. 2nd ed., Kamal Law House, 2012.
11. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians." 2018.
12. Dalmia, Vijay Pal. Indian Cyber Law. LexisNexis, 2017.
13. Duggal, Pavan. Textbook on Cyber Law. Universal Law Publishing, 2014.
14. Dwork, Cynthia. "Differential Privacy: A Survey of Results." Theory and Applications of Models of Computation, Springer, 2008, pp. 1-19.
15. Fatima, Talat. Cyber Crimes. Eastern Book Company, 2011.