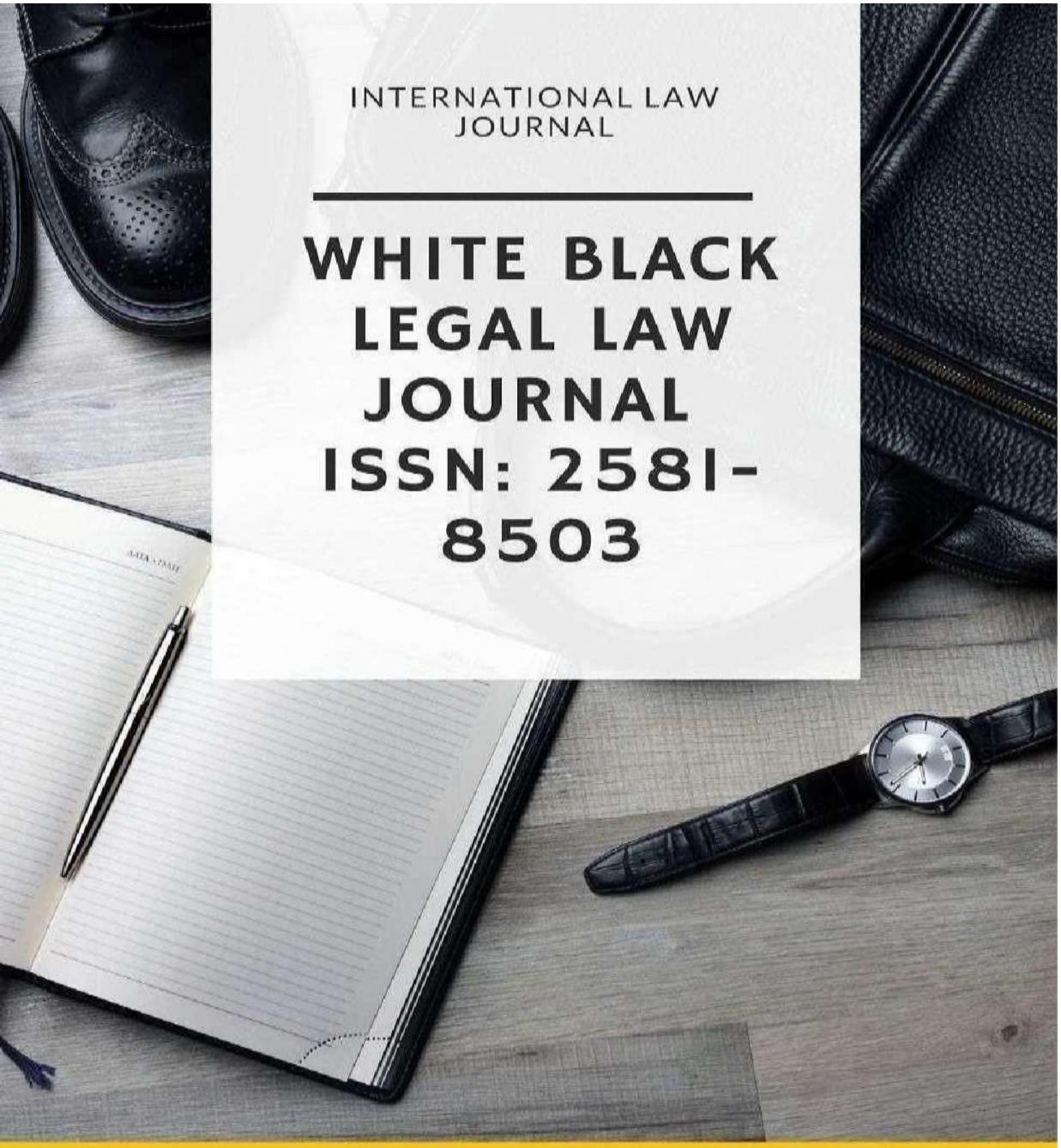

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | July 2025 ISSN: 2581-8503

DATA PROTECTION IN INDIA VIS-A-VIS INTERNATIONAL COUNTRIES

AUTHROED BY - NILAY KUMAR MANI
LL.M from GUJARAT NATIONAL LAW UNIVERSITY

Abstract

Many constitutions across the globe recognise privacy rights as a basic right. Privacy rights are a complex topic. In today's culture, the right to privacy has been recognised by legislation and common vernacular. One of the most fundamental and accepted personal rights is the right to privacy. The Universal Declaration of Human Rights and the International Covenants on Civil and Political Rights both mention privacy rights. The right to privacy is one of the most basic aspects of human life.

Individual data is the new riches of the twenty-first century. It is a person's wealth that, if not properly controlled by the owner, can be transformed into monetary worth for others. Personal data is a big data pool that is still quickly developing, and the business sector is profiting from this trend. For the corporations, this information is seen as a valuable asset. You won't be able to get or manage your personal data from the market once it has become a commodity[1]*. There has been a growing collection of regional and international legislation and policy instruments dealing with the security of information since the late 1970s. Individual data must be gathered honestly and legitimately, according to the law.*

Keywords: *Data Protection, Personal Data, Privacy, Rights.*

Introduction

Data (sometimes sensitive, private, and personal data) communication, transport, storage, and usage have become an integral aspect of present digital transactions. While online transactions are increasingly replacing conventional offline paper transactions as a more convenient and efficient method of dealing, they are not beyond the danger of hacking, data theft, and other cybercrimes. In this borderless digital world, data security has thus become a multi-

[1] Akshaya S, An Analysis of the Data Protection Laws in India, SSRN, 26 June 2020, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3616637>

jurisdictional problem, and nations all over the world have built legislation structures to explicitly address and defend against loss of privacy. In comparison to other jurisdictions, such as the well-established (and often rigorous) data protection rules required by the European Union ("EU"), India's data protection legislation is still in its infancy.

Privacy and Data Protection:

The notion of data protection regulations is well-known throughout the world. The concepts "privacy" and "right to privacy" are difficult to define. It's been used in a variety of ways in various situations. The right to privacy is sometimes used interchangeably with the right to be left alone. A formal connection between groups or individuals is known as privacy. Privacy is a norm, a cultural state, or a situation aimed at individual and community self-realization that varies by civilization. The right to freedom of speech and expression is guaranteed by the Indian Constitution, which states that a person is free to express his or her will and conscience. The European Union has a well-developed data privacy regulation. Private details can only be collected in full accordance with European regulations for legal purposes.

Data protection dictates that information on an individual should not be made available to other people or organisations on an automated basis. Everyone should be able to exert a significant degree of control and usage over his or her data. Data protection refers to the legal safeguards in place to avoid the misuse of personal information obtained through electronic means. It served as a tool for implementing administrative, technical, and physical deterrents to protect personal data. Data protection and privacy are inextricably linked. Individual data, such as identity, address, and phone number, is frequently available at many locations, such as schools, universities, and banks, as well as on a variety of websites. The disclosure of this information to interested parties will constitute to an invasion of an individual's privacy, similar to incessant commercial calls.

Personal Data- Personal data refers to any data that may be used to identify or locate a natural person or an individual. Personal data is any collection of information that links or is gathered together and can lead to the identification of a specific individual. Names and surnames of persons, home addresses, email addresses, and so forth[2].

[2] Christopher Kuner, The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards, 33(1) National Law Review of India (2021)

Data protection- Data protection is a legal term that refers to a statute that protects your personal information. In modern cultures, this regulation allows us to have control over our data and safeguard it from misuse. Data protection rules regulate and limit the operations of businesses and government agencies. These institutions have repeatedly demonstrated that, without any rules restricting their behaviour, they would gather everything, mine everything, retain everything, and share and utilise it with others without informing us anything.

Need for Data protection:

When a person buys anything online, uses a service, pays taxes, enters into a contract or service, registers for email, or goes to the doctor, they must reveal their personal details to do so. This information and data are created and gathered by firms and companies without any interaction with people, even if they are unaware of it. Citizens and customers may only have faith in businesses and governments through statutory law on data protection procedures, which aids in successful legislation to reduce corporate spying and data exploitation. According to reports, 90% of the data on the planet today has been analysed or gathered in the previous two years. As of January 2020, 107 nations throughout the globe have passed data protection laws, and legislation, or were in the process of enacting them. The world appeared to be a totally different place when numerous data protection rules were created. Data protection should guarantee that there are limitations and constraints on the gathering of personal data, as well as that it is gathered and obtained in a legitimate, fair, and transparent manner. Individual data should be collected for specific objectives that are stated at the collection time, and should only be used for those purposes. The processing and collection of individual data should be relevant, appropriate, and restricted to the reasons for which it is received. It is necessary to take steps to verify that the data is current, accurate, and comprehensive. Data should be protected from loss, damage, usage, spillage, exposure, alteration, and unauthorised by others using appropriate security or measures. There should be no hidden data, usage, or other procedures. Individuals must be informed of their personal data, including how it is collected and processed, as well as the objectives for which it is used. People whose data is gathered or obtained must be granted a set of rights that allow them to exercise control over their data and its processing. Those who use or receive such data must be accountable and guarantee that the following values are followed, as well as the laws that entrench these principles.

The Indian Legal System's approach to Privacy and Data Protection:

Information Technology Act, 2000[3] and SPDI Rules-

The Information Technology Act of 2000 ("IT Act"), as well as the rules enacted under it, provides legal principles surrounding data protection, including collection, storage, disclosure, and transfer of electronic data. Offenses such as illegal downloading, destruction, alteration, or deleted records, the emergence of viruses into computers, illegal access to computer systems, theft of data, identity fraud, confidentiality, and release of data in breach of a lawful contract, to name a few, are all punishable by imprisonment and/or fines under the IT Act. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), require a body corporate that processes, deals with, stores, or handles sensitive personal data or information in a computer resource that it owns, controls, or operates to follow certain procedures. The SPDI Rules require a number of critical compliances like acquiring previous written permission from the provider for the purpose of collecting information, but also giving the provider the option of refusing to furnish the information requested and withdrawing his or her consent previously granted in this respect. Make reasonable efforts to ensure that the data source is aware of the fact of collection, the purpose of use, the intended recipients of the data, and the identity of the agency gathering and retaining the data. Private details should not be kept for any longer than is required to achieve the corresponding goal or as required by relevant legislation. Creating and disseminating privacy settings for managing or dealing with personal data. Information may be sent to any other person who provides the same degree of data protection as the SPDI Rules, if it is required for the fulfilment of a legitimate contract with the source of information or if the information provider has given agreement to the transfer. Several additional Indian laws might come into play when it comes to data security, in addition to the IT Act and the SPDI Rules, based on the institution collecting the data and the type of data gathered. Collection of financial information, for example, is generally governed by the Credit Information Companies (Regulation) Act, 2005, and the rules enacted thereunder, as well as Reserve Bank of India circulars released from time to time. Some data security requirements may be found in the Department of Telecommunications' Unified License Agreement for Telecom Service Providers, and the Telecom Commercial Communications Customer Preference Regulations, 2010 have been created to deal with unsolicited commercial communications. The Aadhaar (Data Security) Regulations, 2016, impose an obligation on the Unique Identification Authority of India

[3]

(UIDAI) to have a security policy that sets out the technical and organisational measures that will be taken to keep the information secure, as well as data protection norms for personal information collected under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[4].

A New Data Protection Law on the Horizon:

With a plethora of rules governing the collection and use of various sorts of data, India's data protection structure is still insufficient, and multiple concerns have been expressed about how to further safeguard and appropriately deal with complicated issues such as data loss and privacy. The Indian government, on the other hand, is trying to improve and empower its data privacy protection legislative system. As a result, a Committee of Experts, chaired by former Supreme Court Justice Shri B. N. Srikrishna ("Committee"), has been constituted to research different issues relevant to data protection in India, make specific recommendations on data protection principles, and propose a draught Data Protection Bill. On November 27, 2017, the Committee issued a white paper on a data security structure for India, asking for public feedback. In January of this year, the Committee, in partnership with the Indian Ministry of Electronics and Information Technology, held stakeholder consultation workshops in a number of Indian cities to get their feedback on the problems presented in the white paper. The Supreme Court's landmark judgement in the case of Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.[5], 2017, in which the Court recognized the right to privacy as an integral part of the fundamental right to life and personal liberty under Article 21 of the Indian Constitution, has prompted this white paper. The Court acknowledged that 'informational privacy' is a component of the right to privacy, and that threats to privacy in an era of information might come not just from the state, but also from non-state actors. "Uber owns no vehicles, Facebook creates no content, Alibaba has no inventory, and Airbnb, the world's largest hospitality provider, owns no real estate," according to the Court, "but enterprises like these and other social media network providers, search engines, e-mail providers, and messaging apps, are all additional examples of non-state actors that have a thorough understanding of our exercises, banking transactions, discussions, health and mental state." As people's reliance on internet-based services grows, their digital footprints become increasingly extensive, necessitating unprecedented control of the amount to which those data can be kept, processed, and utilised

[4] Mahak Gandhi and Akshadeep Gupta, A Compendious Analysis: Privacy Protection Laws in India, SSRN, 12 November 2020, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694664>
[5] K.S. Puttuswamy Vs. Union of India, (2017) 10 SCC 1

by non-state entities as well as the government. Because the Government had notified the Supreme Court of the formation of the Committee to evaluate, among other things, data protection laws in the country, the Court considered it necessary to refer the subject to experts so that a solid data protection framework could be put in place. In its white paper, the Committee proposes that the data security structure be based on seven principles: (I) legislation should be adaptable to account for technology changes; (II) law should apply to both government and private sector entities; (III) assent should be legitimate, notified, and impactful; (IV) processing of data should be negligible and only for the objective for which it is decided to seek; and (V) entities controlling the data should be accountable for any data breaches. The Committee is seeking public input on issues such as the territorial applicability of data protection laws, the extent to which the law should apply outside India, such as the inclusion of procedures to ensure compliance by foreign entities, the definition of personal data, the categories of entities that are exempt from certain obligations (e.g., certain actions taken by the state during investigations), the conditions of valid consent, and the exposure of children to online risks.

The Committee also stated that the IT Act's provisions are restricted in their scope and do not appear to address the vast variety of data protection violations that may arise as a result of advances in technology used to handle personal data. Furthermore, the penalties imposed by the IT Act appear to be insufficient and may not serve as a deterrent to developing e-commerce and other technology-based enterprises in India. In response, the white paper detailed the proposed legislation's penalties and adjudicating authority for complaints, as well as noting that compensating an individual who has suffered a loss or harm as a result of the data operator's failure is an essential remedy to be defined within the law. Many aspects of the European Privacy Law, the General Data Protection Regulations, were integrated into the proposed data protection law (GDPR). The bill established legal rules for personal data gathering and usage. Furthermore, the bills provide a set of rights, obligations, and duties for the collecting and management of personal data, as well as a Data Protection Act (DPA) for rules and enforcement of the legal framework. If it is enacted, it will extend to all organisations in India, with the exception of those that are specifically exempted.

Foreign Data Protection Legislation:

General Data Protection Regulation: The General Data Protection Regulation (GDPR) is a strict privacy regulation developed by the European Union in 2016 and implemented on May

25, 2018. It was written to replace the 1995 Data Protection Directive, which was out of date. GDPR strives to ensure that personal data is protected in a uniform manner across EU countries. GDPR's goal is to improve digital security by requiring businesses to preserve EU residents' personal data and privacy by providing them greater control over the personal data they disclose online. It affects enterprises all across the world. Any organisation or website that has the potential to collect personal information from citizens of EU member states must comply with GDPR. The GDPR places a greater emphasis on newer areas like rights to privacy, data protection, data management, and governance. The GDPR also governs the transfer of personal data outside of the European Union[6].

COPPA: The Children's Online Privacy Protection Act (COPPA) is a crucial privacy regulation for children in the United States. This attempts to safeguard the privacy of children under the age of thirteen by limiting the usage and acquisition of personal information about them online. It was enacted by the United States Congress in 1998 and became law in 2000. The Federal Trade Commission of the United States was in charge of enforcing and administering it. It was enacted in particular for online marketers that manage websites on the internet that are primarily accessed by children under the age of 13 and gather private information from such youngsters. The goal of this regulation is to govern how that information is collected. In addition to COPPA compliance, the website operator was obliged to seek verified parental approval from the parents of the children who visited the site prior to collecting or utilising such information. It also extends to firms based or operating outside of the United States that provide services or website access to children in the United States.

CalOPPA: The California Online Privacy Protection Act (CalOPPA) was established to safeguard California residents' privacy rights and personal information. The law became effective on July 1, 2004. It applies to website or online service operators who collect or access personally identifiable information about California residents. If your business, website, or online services have the potential to handle personal information from California citizens, it applies to another nation. The CalOPPA requirements must then be followed by the firm in another nation. This law covers business websites and applications that access mobile and tablet devices[7].

[6] Dan Simmons, 17 Countries with GDPR-like Data Privacy Laws, Comforte Blog, 13 January 2019, available at <https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws >
[7] *Ibid*

HIPAA: The Health Insurance Portability and Accountability Act of 1996 is a federal statute that President Bill Clinton signed in 1996. It is implemented with the goal of ensuring that the privacy and security of patient health information is a top concern for patients, their families, hospitals, healthcare service providers, healthcare professionals, and governments. It necessitated the development of national-level guidelines to safeguard sensitive health-related information without the individual's consent or awareness. The Health Insurance Portability and Accountability Act (HIPAA) apply to businesses that provide healthcare services. It was necessary to strike a balance between maintaining the usage of private details while safeguarding the privacy of patients seeking health treatment and recovery. HIPAA infractions may cost a healthcare company a lot of money in the form of civil or criminal fines.

PIPEDA: The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to businesses in the private sector. It went into effect on April 13, 2000, with the goal of protecting customer personal information acquired by commercial companies. It also protects the consumer's personal information and gives them confidence whenever they share their personal data with private companies via digital services as well as e-commerce. Before collecting, using, or disclosing any personal information, private organisations are required under PIPEDA to get consumer consent. Consumers cannot be denied services or commodities based on whether or not they consent to the acquisition of their personal data.

PDPA: Singapore's Personal Data Protection Act 2012 is a privacy law that was passed by its parliament on October 15, 2012. This will take effect on the 11th of January 2013. This ensures that Singapore's data is protected to the fullest extent possible. It established a minimal standard for the gathering, acquisition, and processing of personal information. It applies to all private sector businesses in Singapore, regardless of size or location. It pertained to the personal information in question, which was gathered in Singapore. The Personal Data Protection Act does not apply to public sector organisations.

19 African nations have passed data security and privacy legislation. Six nations are currently drafting data protection legislation. The remaining nations do not have any data protection or privacy laws. In 2014, the African Union enacted a progressive cyber security and personal data protection treaty. Only 10 nations have signed the pact, and only two countries have approved it.

Data protection and privacy regulations exist in both Australia and New Zealand. In Australia, the government has revised the legislation pertaining to the Australia Privacy Act 1988 to meet the demands of the digital era, including obligatory reporting of any leakage of confidential data to the privacy commissioner and timely notification of impacted consumers. The Privacy Act regulates how businesses acquire, use, keep, disclose, or allow access to personal data in New Zealand. In Asia, 15 nations have data protection and privacy legislation in place, while four more are in the process of creating privacy legislation.

Conclusion:

The current Indian data protection regulatory framework is insufficient to address the significant concerns that have arisen as a result of the government's collection and linking of data, including biometrics, under the Aadhaar Act, as well as the incredibly rapid technological advances and transactions, which raises the risk of data infractions. Recognizing these concerns, the Indian government is trying to find a more efficient legislative framework for data protection, which is being headed by the Committee mentioned above. However, the devil is in the details, and how far relevant modifications and global principles will be introduced, implemented, and enforced in the Indian context remains to be seen. Furthermore, due to its application to Indian organizations that deal with data of EU individuals, the EU's new General Data Protection Regulation, which takes effect in May 2018, is likely to have far-reaching repercussions even in the Indian context. India is not currently recognized by the EU as a nation with an appropriate level of information protection, necessitating additional compliances for data transmission and processing by such Indian organizations[8].

With limited credit facilities, other finance and insurance, a country like India may be forced to make quite different trade-offs between the need for such access and the need for informational privacy. The bill undoubtedly overprotects personal data at a major financial cost by restricting the space for innovation.

The law does not specify what harms the notice-and-consent and data-gathering restrictions clauses are intended to protect users from. As a consequence, they aren't specifically designed

[8] Christopher Kuner, The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards, 33(1) National Law Review of India (2021)

to defend against damages. Furthermore, they run the danger of stifling discoveries that may be beneficial to India[9].

Privacy is a fundamental human right, yet the computer network includes a tremendous quantity of sensitive personal data. Data is not all the same in terms of value and relevance; it varies from one another in terms of utility. Personal data is becoming increasingly valuable and important to businesses all around the world. It is becoming increasingly vital that adequate legislation be enacted to ensure its protection. However, as the cyber world develops, anybody from any part of the globe may access any information pertaining to others at any moment, posing a serious danger to personal and sensitive information. Globalization transforms the entire globe into a computer system, allowing anybody to manipulate any information with a single mouse click. Through different instances, the right to privacy is recognized as a basic right in the constitution, although its protection and application are left to the legislature's discretion. The lack of a strong data protection and privacy law has been a source of worry in recent years. Companies who conduct business in the country but have their data managed and transmitted to another nation have identified this issue as a source of worry. The government is considering the concerns of businesses

[9] Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?, Carnegie India, 9 March 2020, available at <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217>