

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed Edition :

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

IJLRA

EDITORIAL TEAM

EDITORS



Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

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 8 Articles in various reputed Law Journals. Conducted 1 Moot 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.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
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.

RIGHT TO PRIVACY IN LAW OF E-COMMERCE

AUTHORED BY: CHAITANYA DATTA

LLM CCL

CHRIST (DEEMED TO BE UNIVERSITY)

ABSTRACT

In the dynamic environment of e-commerce, where transactions can be carried out smoothly on virtual platforms, the concept of privacy forms the basis of protecting people's personal information from unauthorized entry and abuse. Privacy laws in e-commerce law form an important foundation of the digital age by establishing legal standards, rules, and practices that govern online commerce and interaction with each other. The emergence of the Internet and the growth of digital technology has changed the way business is done, providing convenience and seamless use to consumers around the world. However, this digital revolution also brings challenges to protecting individual privacy in cyberspace. As the amount of personal data generated by the processing of online activities, from tracking behavior to financial transactions, increases, concerns about data privacy, security breaches, and unauthorized access are becoming increasingly common. In response to these challenges, international legal systems are seeking to develop strong mechanisms to protect privacy rights in e-commerce. These processes include legal frameworks, policies, and industry standards designed to regulate the collection, storage, processing, and sharing of personal data by e-commerce sites. Privacy in e-commerce goes beyond just regulatory compliance; It covers general concepts such as self-control, reputation, and trust in the digital economy. Self-insured privacy policies can increase consumer trust, improve online security, and support data management for e-commerce participants. It is also responsible for the innovation and transparency that drives the development of privacy-enhancing technologies and applications that impact consumer design. In the complex field of e-commerce, the right to privacy has emerged as an important human right that is important to promote fairness, justice and trust in the digital ecosystem. As e-commerce continues to evolve and expand its scope, protecting privacy rights remains a priority, reinforcing the idea that privacy is not just a legal right but the essence of human dignity and freedom in the digital age.

KEYWORDS

E-commerce, Privacy, Digital age, Personal data, Regulations, Trust

1. INTRODUCTION

In the era of rapid technological advancement and digital transformation, e-commerce has become a major force in business development worldwide. E-commerce in India has witnessed unprecedented growth, driven by factors such as increasing internet penetration, smartphone adoption, and government digital economic measures. However, the important thing to consider in this digital revolution is the protection of personal privacy in the field of e-commerce. The right to privacy is a human right defined in many international agreements. Treaties, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In the context of e-commerce, privacy refers to the protection of personal information shared by users across e-commerce platforms and organizations during online transactions, interactions, and collaborations. This includes but is not limited to important information such as financial information, contact information, search history, and purchasing preferences. In India, the legal framework regulating e-commerce and privacy has evolved to adapt to the changing digital environment and solutions to emerging problems have been provided. The Information Technology Act of 2000 and its subsequent amendments form the basis of regulations regarding electronic commerce and the protection of private information in the country. In addition, the enactment of the Personal Data Protection Act 2019 further demonstrates the government's commitment to creating a data protection system that meets international standards. However, despite the law, there are still many difficulties in implementing privacy rights in e-commerce. Issues such as data breaches, unauthorized access to personal data, and privacy laws continue to pose risks to consumer privacy and security information. Additionally, the power of technology requires constant vigilance and preventive measures to mitigate threats and vulnerabilities.

In this context, it is important to evaluate the current legal framework regulating privacy in e-commerce and explore ways to improve its performance. This article focuses on the relationship between law, technology, and privacy in the e-commerce industry in India. - trade. environment. The e-commerce ecosystem gives customers trust and confidence.

2. RIGHT TO PRIVACY

Privacy is the right to be left alone or to be free from the misuse or abuse of one's identity. The right to privacy protects individuals against undue notoriety, seclusion, and intervention by the

public in areas over which they have no voice or involvement. It is the right of a person to be free from intrusion into or publicity concerning matters of a personal nature.¹ The right to privacy stems from Article 21 of the Indian Constitution, which declares that "No person shall be deprived of his life or personal liberty except pursuant to the procedure established by law." Although the 'right to privacy' is not explicitly recognized in the Indian Constitution, it is inherent in Article 21, as evidenced by court rulings. Several legal rulings have addressed the concept of privacy. These legal rulings helped establish the "Right to Privacy" as a fundamental right.

The right to privacy in India has been widely recognized through interpretation and jurisprudence, especially following a landmark judgment by the Supreme Court in India in 2017. *Puttaswamy and Anr. v. The Union of India*² has found that the right to privacy is a fundamental right protected by the Constitution of India. Before this decision, the right to privacy was unclear in India; courts often referred to this as an implied right derived from other important rules. However, the Puttaswamy judgment clearly recognized the right to privacy enshrined in the fundamental rights enshrined in the Constitution of India, especially from the perspective of Article 21 which guarantees the right to life and personal liberty. This important decision had a significant impact in many areas, especially data protection, surveillance, personal freedom, and the freedom of the individual. Subsequently, the government of India took steps to legislate on data protection and privacy-related issues by promulgating the Privacy Act 2019, which aims to regulate the processing of personal data and establish a data protection system.

In general, the right to privacy as a fundamental right in the Indian sphere recognition is important in the law of the country; It provides people with greater protection and freedom over their personal information and privacy.

3. WHAT IS E-COMMERCE

Electronic commerce or e-commerce refers to a wide range of online business activities for products and services. It also pertains to "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact."³ E-commerce refers to online transactions that include transferring ownership or rights to products or services over a computer-mediated network.

Although widely used, this description does not fully encompass current advancements in this

¹ Kumar, Rahul, *Jurisprudence of Right to Privacy in India* (July 30, 2020). Available at SSRN: <https://ssrn.com/abstract=3664257>

² (2017) 10 SCC 1

³ Gupta, A., 2014. *E-Commerce: Role of E-Commerce in today's business*. International Journal of Computing and Corporate Research, 4(1), pp.1-8.

innovative business model. E-commerce refers to the use of electronic communications and digital information processing technologies in commercial transactions to build relationships and produce value for organizations and people. E-commerce and e-business are not the same thing. E-commerce utilizes information and communications technology (ICT) for both inter-business and business-to-consumer transactions. In contrast, with e-business, information and communication technology is employed to improve one's business. This term refers to any procedure carried out by a corporate organization, whether for-profit, governmental, or non-profit, using a computer network. E-business refers to the use of new economy technologies, ideas, and computer paradigms to enhance an organization's processes and provide added value to customers.

There are many different types of e-commerce, each addressing specific business and customer needs. In this article, we will take a closer look at the different types of e-commerce, including business-to-business (B2B), business-to-consumer (B2C), business-to-government (B2G), and consumer-to-business (B2G). -consumer (C2C).

- **Business-To-Business (B2B)**

B2B e-commerce, or business-to-business e-commerce, involves business between companies, rather than between companies and consumers. Logistics includes many products, including service providers, outsourcing services, auction solutions, content management software, and web-based commerce providers. E-commerce is an online platform where buyers and sellers interact and do business. These e-commerce sites facilitate effective communication and commerce between businesses, making the process faster and more efficient. In general, B2B e-commerce plays an important role in improving the efficiency and effectiveness of business relationships and business in the digital age.

- **Business-To-Consumer (B2C)**

Business-to-consumer (B2C) e-commerce involves transactions between companies and individual consumers. In this model, customers gather information, purchase physical goods like books or consumer products, or acquire digital goods such as software or e-books over electronic networks. B2C e-commerce offers several benefits, including reducing transaction costs by providing consumers with easy access to information and competitive pricing. Additionally, it lowers market entry barriers since setting up and maintaining a website is more affordable than establishing physical stores. Particularly for digital goods, B2C e-commerce is advantageous as

it eliminates the need for a physical distribution network. As internet usage grows in countries, the delivery of digital goods becomes increasingly viable.

- **Business-To-Government (B2G)**

Business-to-government (B2G) e-commerce involves transactions between companies and governmental entities. It encompasses the use of the Internet for various government-related activities such as public procurement and licensing procedures. B2G e-commerce is characterized by the public sector taking a leading role in implementing electronic commerce initiatives, driven by the need to enhance the efficiency of procurement systems. By adopting web-based purchasing policies, B2G e-commerce aims to increase transparency in procurement processes and mitigate the risk of irregularities. However, despite its potential benefits, the B2G e-commerce market remains relatively small compared to overall e-commerce, mainly due to underdeveloped government e-procurement systems.

- **Consumer-To-Consumer (C2C)**

Consumer-to-consumer (C2C) e-commerce involves transactions conducted directly between private individuals or consumers. This type of e-commerce is characterized by the proliferation of electronic marketplaces and online auctions, particularly in niche industries where individuals can bid for goods or services from various suppliers. C2C e-commerce holds significant potential for creating new markets and facilitating peer-to-peer transactions. On the other hand, consumer-to-business (C2B) transactions entail reverse auctions, empowering consumers to initiate and drive transactions. While there is limited data available on the exact size of the global C2C e-commerce market, popular platforms like eBay and Napster generate substantial sales volumes, indicating the considerable scale of this market segment.

4. CHALLENGES OF RIGHT TO PRIVACY IN E-COMMERCE IN INDIA

The Indian e-commerce industry is booming, with a projected value of US\$350 billion by 2025. However, this rapid growth has also posed new challenges, particularly in the area of data privacy.⁴ E-commerce businesses acquire a large quantity of personal information from their customers, such as names, addresses, contact information, payment information, and browsing histories. This information is critical for businesses to run smoothly and give personalized

⁴ Mansi Javiya, *Data Privacy in Indian E-commerce: Contractual Challenges and Legal Solutions*, Into Legal World, Dec 15, 2023

services to their clients. However, it does create severe privacy concerns. This data is frequently utilized for marketing reasons, but it may also be used for fraud detection and risk assessment.

In recent years, multiple high-profile data breaches at Indian e-commerce sites have exposed the personal information of millions of consumers. This has resulted in heightened scrutiny of e-commerce enterprises' data privacy policies. Obtaining users' consent for the collection and processing of their personal data is important for protecting their privacy. However, many e-commerce companies have privacy policies and service promises that may not be easy for users to understand. Being transparent and clear about how personal information is collected, used, and shared is a complex issue that requires management and control. E-commerce platforms often transfer personal data across borders for a variety of purposes, such as cloud storage, data analysis, and customer support. However, this cross-border transfer of data has raised concerns in India and other countries about evidence, jurisdictional issues, and data protection policy compliance issues.

International harmonization of data protection standards and regulations poses major challenges for e-commerce companies operating in a global environment. E-commerce platforms often enable user profiling and advertising campaigns based on customer browsing and purchasing behavior. While personalized recommendations can improve user experience, they also raise privacy concerns about how users' data could be identified and monetized without explicit agreement. It is still difficult to measure the satisfaction of e-commerce companies regarding users' privacy rights. E-commerce companies must obtain consent from users before collecting and using their personal data. However, there have been concerns that some e-commerce companies are not obtaining consent properly or that they are using consent to justify the collection of more data than is necessary.⁵

5. LEGISLATIONS IN INDIA REGARDING THE PROTECTION OF DATA IN E-COMMERCE IN INDIA

Government initiatives such as Startup India, Digital India, the allocation of funds for the BharatNet Project, the promotion of a “cashless economy,” and the launch of the Unified Payment Interface by the RBI and the National Payment Corporation of India have all contributed to the

^{5 5} Mansi Javiya, *Data Privacy in Indian E-commerce: Contractual Challenges and Legal Solutions*, Into Legal World, Dec 15, 2023

country's e-commerce sector's growth and success.⁶

The e-commerce landscape in India includes regulatory frameworks, technology, data protection information, foreign investment, tax, consumer protection, intellectual property rights, etc. It is subject to various laws and regulations covering many issues, including: This legal framework is important for ensuring fair competition, protecting consumer interests, and promoting the development of e-commerce, as well as solving new problems such as cyber security and judicial review.

The Foreign Direct Investment (FDI) Act, the Foreign Direct Investment Act (FEMA) 1999, and the Companies Act 2013 have laid the foundations for regulating foreign direct investment in e-commerce and ensuring compliance with trade rules. regulations. FDI policy differs between business type and commodity type: the former automatically allows 100% FDI, but the latter has banned FDI. In addition, the law determines the conditions for foreign direct investment into the country, where equivalent foreign investment in retail trade and wholesale cash and transportation has internal trade protection.

The Payment and Payment Systems Act, 2007, and other regulations issued by the Reserve Bank of India (RBI) regulate payment systems in e-commerce and ensure the security and functioning of online payments. E-commerce companies must follow the RBI guidelines to implement the payment process and manage the money node to process payments on their platforms. Regulatory and packaging laws, including the Audit Act 2009 and the Audit (Packaged Goods) Act 2011, require e-commerce businesses to provide factual information about the products they sell online. These regulations require a detailed description of the product, including its dimensions, weight, and other attributes, to ensure consumers are safe and transparent in the marketplace.

Sales, deliveries, returns, and refunds in e-commerce are governed by the following laws: The Sales Act 1930 outlines the rules and procedures. Responsibility of both parties to the business. E-commerce platforms should provide clear sales and shipping information, including confirmation information, details, and return/refund options to increase customer trust and satisfaction. The Indian Contract Act, of 1872 and the Information Technology Act, of 2000 (IT Act) govern electronic contracts and create legal frameworks for online transactions. Digital signatures, electronic documents, and due diligence are key elements of the IT Act to ensure the

⁶ Yuktha, *E-Commerce Laws And Regulations In India*, Vakil Search, 26 December 2023

efficiency and security of electronic commerce. Data protection and privacy issues in e-commerce have been addressed by the IT Act and India's General Data Protection Regulation (GDPR) has come into force. 2018. E-commerce sites must comply with data privacy and data protection. Laws to ensure the security and confidentiality of data used to protect private customers. Intellectual property issues, including trademarks and copyrights, require e-commerce businesses to have appropriate rights over the products and content they sell online. Although India has strong intellectual property laws, issues such as fraud and litigation are a constant concern, with legislation and regulations constantly needing to be updated to adapt to the changing e-commerce landscape.

6. SUGGESTIONS

Developing data protection rules involves changing existing rules and regulations to respond to changes in e-commerce and digital marketing. This requires a comprehensive personal data service across all e-commerce businesses, regardless of their size or location. Clear guidelines for data collection, storage, processing, and sharing should be established to ensure user privacy is a priority at every step. By implementing stricter rules, the risk of privacy breaches can be reduced and users can feel safer sharing their information online. Allowing users to opt-out is important to ensure individuals have control over their personal information. E-commerce platforms need to be transparent about the types of data they collect, how they use it, and with whom they share it. Users should have the ability to determine the confidentiality of their information and the option to opt out of information sharing if they wish. By prioritizing user agreement and transparency, trust between users and e-commerce companies can be strengthened, leading to online security.

Controlling the use of encryption methods Strong authentication measures are required to prevent data transmission and storage in e-commerce. Encryption helps protect sensitive data from unauthorized access or interception during transmission, and secure authentication methods such as multiple authentication help prevent unauthorized access from illegal spending. By implementing encryption and secure authentication, e-commerce platforms can reduce the risk of privacy breaches and unauthorized access to user information. Perform necessary security audits to ensure e-commerce businesses comply with privacy laws and business standards. These reviews help identify vulnerabilities or security weaknesses, allowing the platform to resolve the issue before a breach occurs. Penalties for non-compliance with privacy laws create an incentive

for platforms to prioritize data security and invest in security measures. By regularly reviewing security and ensuring compliance with privacy laws, e-commerce platforms can ensure a high level of security and protect user privacy.

Encouraging e-commerce platforms to adopt data minimization practices, including collecting only necessary information that is necessary for the business. This reduces the impact of leaks by reducing the amount of sensitive data stored. Additionally, promoting the anonymity of user data anywhere can help protect personal privacy while also supporting data identification for businesses. By minimizing the amount of data collected and not disclosing the user's information, e-commerce platforms can reduce privacy risks and protect the user's privacy.

The lack of a specific time frame for reporting data breaches in Article 8, Article 6 of the Data Protection and Privacy Act is a key factor that will cause data fiduciaries to delay or conceal the crime. Compared to the GDPR's strict reporting window, we need clear timelines to provide timely and transparent breach notifications to ensure accountability and reduce risk. While DPDP Act also allows companies to decide on security controls, it does not provide the opportunity to implement security in a similar way to self-monitoring. It is important to implement security checks on third parties and strengthen data protection, as in other countries, especially in sectors such as fintech and healthcare. While the bill has personal in its name yet the only definition we get of personal data from the bill is — *“any data about an individual who is identifiable by or in relation to such data”*⁷. The lack of clarity in defining personal data within the DPDP raises concerns about the inclusion of various types of sensitive information like images, audio, metadata, etc. without clear demarcation. This ambiguity could lead to organizations downplaying breaches by claiming leaked data isn't personal. Implementing clear categorization and separate governance for sensitive, confidential, PII, and public data is crucial to mitigate this loophole and ensure comprehensive data protection.

7. CONCLUSION

In conclusion, privacy policy in e-commerce law is important for protecting trust, security, and integrity in the digital economy. As e-commerce continues to evolve and expand, it is still

⁷ Piyush Goyal. Medium, *7 major shortcomings of Digital Personal Data Protection Act, 2023*, 17th August 2023, <https://medium.com/@piyushgoyal2021/7-major-shortcomings-of-digital-personal-data-protection-act-2023-7ec16368332e>

important to protect privacy rights to ensure the integrity of online transactions and increase customer trust. While existing legal frameworks such as India's Information Technology Act and Data Protection and Privacy Act 2023, have laid the foundation for regulating e-commerce and protecting personal data, there are still problems and areas for improvement. To solve these problems, it is necessary to implement stricter data protection laws, improve user agreement and transparency, adopt encryption and security measures, conduct regular security audits, support data reduction and anonymity practices, and monitor the importance of security. education. and awareness programs. Collaboration between regulators, market participants, and e-commerce companies is also important to address privacy concerns and develop effective solutions.

In general, it is very important to prevent privacy problems in e-commerce and produce effective solutions. In any case, protecting privacy rights in e-commerce is not only a legal issue; Morality is important. By embracing privacy protection and promoting a culture of privacy, e-commerce can continue to thrive while supporting human rights in the digital age.

8. REFERENCES

- Mansi Javiya, *Data Privacy in Indian E-commerce: Contractual Challenges and Legal Solutions*, Into Legal World, Dec 15, 2023
- Yuktha, *E-Commerce Laws And Regulations In India*, Vakil Search, 26 December 2023
- Justice K.S. Puttaswamy Vs. Union Of India, <https://translaw.clpr.org.in/case-law/justice-k-s-puttaswamy-anr-vs-union-of-india-ors-privacy/>
- Kumar, Rahul, *Jurisprudence of Right to Privacy in India* (July 30, 2020). Available at SSRN: <https://ssrn.com/abstract=3664257>
- Gupta, A., 2014. E-Commerce: Role of E-Commerce in today's business. *International Journal of Computing and Corporate Research*, 4(1), pp.1-8.
- Piyush Goyal. Medium, 7 major shortcomings of Digital Personal Data Protection Act, 2023, 17th August 2023, <https://medium.com/@piyushgoyal2021/7-major-shortcomings-of-digital-personal-data-protection-act-2023-7ec16368332e>