INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

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

ISSN: 2582-6433

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 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.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

DATA PRIVACY IN THE AGE OF DIGITAL COMMERCE: BALANCING BUSINESS NEEDS AND CONSUMER RIGHTS.

AUTHORED BY - RAHUL SHANTINATH SOLLAPURE

ABSTRACT

Data privacy is a growing concern in the age of digital commerce. Businesses collect and use vast amounts of data about their customers, and consumers are often unaware of how their data is used. This can lead to several risks, including identity theft, fraud, and discrimination. This research paper will explore the challenges and opportunities of data privacy in digital commerce. It will begin by examining the legal and regulatory landscape governing data privacy. It will then discuss the ethical implications of data collection and use. Finally, it will explore best practices for data protection and security and the role of technology in protecting consumer privacy.

The age of digital commerce has ushered in a new era of data collection and processing. While this has brought about many benefits for businesses and consumers, it has also raised new challenges regarding data privacy. Businesses need to collect and use data in order to operate effectively, but consumers have a right to privacy and control over their own data. Consumers of digital goods and services are less protected than consumers of traditional goods and services. This is because digital goods and services can be complex and challenging to understand, and consumers may have less recourse if harmed. This research topic will explore the challenges and opportunities of balancing business needs and consumer rights in the age of digital commerce. It will examine the legal and regulatory landscape governing data privacy and the ethical implications of data collection and use. It will also explore best practices for data protection and security and the role of technology in protecting consumer privacy. The research topic will provide valuable insights into balancing the competing interests of businesses and consumers in the age of digital commerce.

Keywords: data privacy, digital commerce, business needs, consumer rights, data protection, data security, data ethics.

ISSN: 2582-6433

INTRODUCTION:

As consumers adopt digital technology faster, the data they produce gives businesses the chance to better engage with their customers and the duty to protect their personal information. Numerous businesses, for instance, use data better to understand their customers' needs and pain points. These data, which include location tracking and other types of personally identifiable information, are of great value to businesses. Information privacy is controlling how one's personal information is obtained and used.[1] In e-commerce transactions, consumers do not have control over the collection and use of their information as websites (firms) knowingly and/or wilfully collect information from consumers without their knowledge and consent through the use of cookies, web bugs, etc. This unauthorised access and collection is done with the aim of a) capturing consumers' needs and b) marketing to them. The main issue with e-commerce transactions is that a) e-commerce businesses are required to collect customers' and visitors' information[2] because their marketing strategies depend on consumers' information and behaviour in e-commerce transactions, and b) from the perspective of consumers, this is an infringement on their information privacy or data privacy.[3] Thus, users' privacy concerns about protecting their personal information on commercial websites are growing as a result of the information collection by e-commerce websites on the one hand and the loss of information privacy (i.e. control over the collection, use, storage, processing, dissemination, and likely chances of misuse) on the other.[4] Some legal policies and regulations have already been established at the international and national level to address the challenges of information privacy in e-commerce and to promote legal control over privacy protection in electronic transactions. At the international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement, etc., are directed to be followed by e-commerce companies to ensure information privacy in the conduct online. At the national level, countries worldwide have enacted different laws to protect the privacy of individuals. A Business Week/Harris Poll survey[5] found that over 57% of online buyers want some legal regulations to control the use and disclosure of their information by e-commerce websites and protect information privacy.

[1] White, T. B., Consumer Disclosure and Disclosure Avoidance: A Motivational Framework, Journal of Consumer Psychology Vol. 14, 41-51 (2004).
[2] Bessen, J., Riding the Marketing Information Wave, Harvard Business Review Vol. 71, No. 5, 150-160 (1993).
[3] Culnan, M. J. & Armstrong, P. K., Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation, Organization Science, Vol. 10, No. 1, 104-115 1999.
[4] Featherman, M. S. & Pavlou, P. A., Predicting E-Services Adoption: A Perceived Risk Facets Perspective, International Journal of Human-Computer Studies, Vol. 59, No. 4, 451-474, (2003).
[5] Harris Poll, Privacy and American Business Press Release (online) (June 24, 2015), http://www.epic.org/privacy/survey/.

ISSN: 2582-6433

CONCEPTUAL FRAMEWORK:

What is Data Protection?

The law intended to secure your data is known as data protection. Data protection rules must constrain and mould the actions of businesses and governments to give us, the people in modern societies, the power to control our data and safeguard it against misuse. These organisations have demonstrated time and time again that they will do everything in their power to gather, mine, retain, and distribute the resources while keeping us in the dark.

Why is Data Protection Needed?

You have to provide personal information each time you use a service, buy anything online, set up an email account, go to the doctor, file your taxes, or finish any contract or service request. Even without your knowledge, businesses and organisations that you are unlikely to have ever actively interacted with are creating and gathering data and information about you. When businesses and the government follow sound data protection procedures and enact laws that effectively reduce corporate and governmental surveillance and data exploitation, citizens and consumers can feel confident in both.

People began to wonder what happened to their data after providing it once data collection and processing became commonplace. Who was authorised to access the information? Was it kept accurate? Was it being collected and disseminated without their knowledge? Could it be used to discriminate or violate other fundamental rights?

From all these questions, and amid growing public concern, data protection principles were devised through numerous national and international consultations.

The German region of Hesse passed the first law in 1970, while the US Fair Credit Reporting Act 1970 also contained data protection elements.[6] The US-led development of a 'code of fair information practices' in the early 1970s continues to shape data protection law today. At roughly the same time, the UK established a commission to investigate risks by private firms, which came to similar conclusions.

[6] Robert Gellman, 'Fair Information Practices: A Basic History', April 2017, available [PDF] at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

ISSN: 2582-6433

Strong data protection measures can limit data exploitation, stop destructive data practices, and give people more power. Establishing the required governance frameworks on a national and international level is essential to guaranteeing that people have significant rights over their data, that those processing personal data (in both the public and private sectors) are subject to strict obligations, and that those who violate these obligations and protections can be held accountable.

Data Protection in Practice Today

Over 100 nations worldwide have comprehensive data protection laws in place as of January 2018, and another 40 or so are in the process of doing so. Other nations might have specific privacy rules that apply to things like children's records or financial information, but they lack a comprehensive data protection law. When data protection is governed in all nations without a comprehensive framework, it is done so through sector-specific regulations. Although the US Privacy Act of 1974 was a pioneer in the field of data protection, it only applies to the Federal Government. Subsequent laws, like the Children's Online Privacy Protection Act (COPPA), apply to particular industries or demographic groups. However, no comprehensive data protection law is in place now. Many nations still use this sectorial strategy, including India. The approval of the EU General Data Protection Regulation (GDPR), which will go into effect on May 25, 2018, marked a significant advancement in data protection law. The GDPR is extensive and covers practically every processing of personal data. A new development occurred in May 2018 with the revision to the Convention for the Protection of Individuals with respect to the Automatic Processing of Personal Data (No. 108) of the Council of Europe. Since its introduction in 1981, more than 40 European nations, including nine non-Council of Europe members, have utilised the Convention as a base for their individual data protection policies. The updated version of the Convention recognises current ideas and adds new rules to strengthen them. Obligations, responsibility, and methods of enforcement.[7] To learn more about data protection regulations organised by the nation, see the in-depth reports from Privacy International.[8]

[7] Council of Europe, 'Modernisation of Convention 108', Council of Europe Portal, available at https://www.coe.int/en/web/data-protection/convention108/modernised
[8] Privacy International, 'State of Privacy', available at https://www.privacyinternational.org/reports/state-of-privacy

ISSN: 2582-6433

LEGAL REGIME/ JUDICIAL PERSPECTIVE:

Data Privacy in Digital Commerce: Indian Legal Perspective

Privacy is closely connected to data protection in the information and communication technology-equipped society.[9] Individual data like his name, telephone number, profession, family, choices, PAN card number, credit card details, social security number, etc., are disclosed in the electronic transactions and then are available on various websites. Unauthorised access, collection, use, misuse, relocation, and transmission of the information to a third party ultimately result in the invasion of individuals' privacy, even though authorised data collection and storage may only increase the likelihood of information privacy loss. Accordingly, issues with privacy in electronic transactions may stem from incorrect management of information flow. In addition to defining what privacy is, how it should be valued, and how much legal protection it should receive, the law also establishes authorised protections for situations in which people can value their privacy and guard against unauthorised entry by others.

Data Protection: Essential for Exercise of Right to Privacy

Privacy is an internationally recognised human right. Article 12 of the Universal Declaration of Human Rights (UDHR) proclaims that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence .... Everyone has the right to the protection of the law against such interference or attacks".[10]

The UDHR has formed the basis for the major international human rights treaties, which enshrine the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR) in Article 17.

Data security and privacy are inextricably related. People must have the resources and instruments necessary to exercise their right to privacy and safeguard their personal information against misuse in their capacities as citizens, clients, and consumers. The responsibilities of those handling data must be unambiguous for them to safeguard personal information, minimise disruptions to the right to privacy, and be held accountable for noncompliance. This is especially true about our personal information. As elaborated below, personal data is any information of an

[9] Philip E. Agre & Marc Rotenberg, Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press. USA. (1997) (May 27, 2015), http://polaris.gseis.ucla.edu/pagre/landscape.html
[10] GA Res. 217 (III) A, UDHR, art. 12 (Dec. 10, 1948)

ISSN: 2582-6433

individual that is processed automatically or stored in a structured file system. The goal of data protection is to preserve our inalienable right to privacy by controlling the use of personal information, giving people control over their data, and establishing clear responsibility guidelines and accountability frameworks for those who handle or process data.

Data Protection: A Right?

It has long been acknowledged that one of the core components of the right to privacy is protecting personal data. It has gained recognition as a stand-alone right recently. For instance, under Article 8 of the Charter of Fundamental Rights of the European Union (2012/C 326/02), data protection is now recognised as a separate right in addition to Article 7, which protects the right to privacy.

Many nations have constitutional rights to habeas corpus, which safeguards an individual's personal information by allowing them to view the information that is kept about them and allowing them to file a complaint with the Constitutional Court.

Information Technology Act, 2000 and Data Privacy: An Analysis

The Indian legislature passed the Information Technology Act of 2000 to comply with UNCLTRAL's (the United Nations Commission on International Trade Law) requirements, adopt a model law on electronic commerce, and give legal recognition to transactions made using electronic data interchange and other forms of electronic communication, also known as electronic commerce.[11]

The Act was therefore created for the reasons listed below[12]: 1) Promote the growth of e-commerce; 2) Ensure the regulatory environment for the security of e-commerce; and 3) Provide a legislative framework for the regulation of electronic contracts, security, and integrity of electronic transactions. (This legal framework will directly impact the expansion and development of e-commerce), 4) to facilitate and validate the use of digital signatures for authenticating electronic records, 5) to support the expansion of the Indian IT sector globally, 6) to ensure the security and privacy of electronic transactions, and 7) to draw foreign direct investment (FDI) in the information technology sector.

[11] The Information Technology Act, 2000, (May 26, 2012), http://www.aicteindia.org/downloads/itact2000.pdf.
[12] Nasir M. Ali, Legal Issues involved in E-commerce, Ubiquity (Mazgine), New York, NY, USA (2004) (May 28, 2015), http://ubiquity.acm.org/article.cfm?id=985607.

ISSN: 2582-6433

(A)Provisions about data protection & personal data protection

In the Information Technology Act of 2000, the concept of 'personal data' was not discussed. It defines 'data but does not provide any definition of personal data. Furthermore, the definition of data is provided with more relevance to cybercrime.[13] Hence, there is confusion among the researchers about whether the Indian IT Act of 2000 deals with data protection or with 'personal data protection' as well.

(B) Civil Liability in case of data, computer database theft, privacy violation, etc[14]

Cybercrime is covered in detail in Chapter IX of the Information Technology Act 2000. Sections 43(a) through 43(h) encompass a wide range of cyber offences, including unauthorised access to computers, computer systems, computer networks, and resources. Section 43 of the Act addresses several issues, including civil liability against the offender and the payment of damages (up to one crore rupees) to the person adversely affected by the specified events. These incidents include (a) invasions of privacy, trespassing on computers, etc. (b) Theft of data housed or stored on any media; digital copying, downloading, and extraction of data, computer databases, or information (c) Computer disruption, data contamination, etc. (d) Data corruption, loss, etc. (e) Interruptions to computer data or databases, spam, etc. (f) Data theft, fraud, forgeries, denial of service attacks, etc.It is crucial to stress that compensation for these broad categories of cyber infractions can only be given when someone is injured by access, disruption, denial, etc.

ANALYSIS

The age of digital commerce has ushered in a new era of data collection and processing. Businesses collect and use vast amounts of data about their customers, and consumers are often unaware of how their data is used. This can lead to several risks, including identity theft, fraud, and discrimination. Businesses need to collect and use data to operate effectively. For example, companies use data to understand customer needs, develop new products and services, and target advertising. However, consumers have a right to privacy and control over their data. There are many challenges to balancing business needs and consumer rights in the age of digital commerce. One challenge is that the legal and regulatory landscape is constantly evolving. It can be difficult for businesses to keep up with the latest changes, and consumers may not be aware of their rights.

[13] The Final Report: The First Analysis of the Personal Data Protection Law in India, Prepared by CRID-University of Namur, Report delivered in the framework of contract, JLS/C4/2005/15 between CRID and the Directorate General, Justice, Freedom and Security. (May 29, 2015), http://ec.europa.eu/justice/data-protection/index_en.htm.
[14] Sharma, Vakul, Information Technology-Law & Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd (2004)

ISSN: 2582-6433

Another challenge is that data is often collected and processed without consumers' knowledge or consent. For example, businesses may track users' online activity through cookies or other tracking technologies. Consumers may not be aware that their data is being collected, and they may not have a choice about whether or not their data is shared with third parties. There are several steps that can be taken to balance business needs and consumer rights in the age of digital commerce. One step is to develop clear and transparent data privacy policies. These policies should explain what data is collected, how it is used, and with whom it is shared. Consumers should also be allowed to opt out of data collection and sharing. Another step is to implement strong data security measures. Businesses should protect consumer data from unauthorised access, use, disclosure, disruption, modification, or destruction.

Finally, consumers must be educated about their data privacy rights and how to protect their data. Consumers should be aware of the different ways that their data is collected and used, and they should take steps to protect their data, such as using strong passwords and being careful about what information they share online.

It is crucial for individuals to take steps to protect their data proactively. This includes implementing robust cybersecurity practices, such as utilizing strong and unique passwords, employing multi-factor authentication, and exercising caution regarding the information they share online. Educating consumers on these preventive measures is paramount in mitigating potential risks associated with unauthorized access and data breaches.

Furthermore, promoting digital literacy ensures that consumers are equipped to navigate the complexities of the online world. Understanding the implications of data sharing and the value of their personal information empowers individuals to make conscious choices in their online activities.

In essence, a well-informed consumer base is better equipped to safeguard their data privacy rights, contributing to a more secure and responsible digital environment. As technology continues to advance, ongoing education remains a cornerstone in fostering a culture of privacy-conscious users who actively participate in shaping a safer digital future.

ISSN: 2582-6433

CONCLUSION

The discussion above makes it clear that even while the government is careful to update the law on data privacy in a timely manner, the current proposed bill does not appear suitable for preserving data privacy with a vision to ensure growth in digital commerce. As a result, the Privacy Bill seems to lack clarity and coherence when viewed as a whole piece of privacy protection legislation. It needs a thorough evaluation, clarification, and additions for improved and balanced data privacy protection with inclusive e-commerce expansion.

The Privacy Bill, as presently formulated, is criticized for its perceived lack of clarity and coherence, posing challenges for comprehensive privacy protection. A thorough evaluation is imperative to address these concerns, involving the identification and rectification of ambiguities and gaps in the legislation. It is crucial to enhance the bill's effectiveness by introducing clarifications and additions that align with the evolving landscape of digital transactions.

Striking a balance between privacy safeguards and the facilitation of inclusive e-commerce expansion is pivotal. An improved and well-defined Privacy Bill is essential to instil confidence among users, businesses, and stakeholders alike. By addressing these shortcomings through careful evaluation and necessary amendments, policymakers can ensure that the legislation not only meets the current demands of data privacy but also fosters a conducive environment for the sustained growth of digital commerce.

SUGGESTIONS:

Policymakers and regulators are increasingly recognizing the critical need to empower consumers in the digital environment through various strategic initiatives. One crucial aspect involves developing educational programs aimed at enhancing consumers' understanding of their rights in the digital space. By fostering digital literacy and awareness, individuals can make informed decisions, safeguarding their privacy and navigating the complexities of the online world.

Promoting the use of privacy-enhancing technologies is another pivotal strategy. Encouraging the adoption of tools and technologies that prioritize consumer data protection helps build a more secure digital landscape. This involves advocating for robust cybersecurity measures and promoting the integration of privacy features into digital products and services.

ISSN: 2582-6433

Additionally, policymakers are focusing on establishing effective mechanisms for consumers to report and resolve disputes with digital businesses. Implementing accessible and transparent processes for conflict resolution enhances consumer trust and ensures fair treatment in the digital marketplace. Creating platforms for reporting issues and facilitating resolution mechanisms strengthens the regulatory framework, fostering a more accountable and consumer-centric digital ecosystem.

In sum, these strategies reflect a comprehensive approach to address the challenges posed by the digital environment, aiming to empower consumers, protect their privacy, and establish mechanisms for fair and efficient dispute resolution in the ever-evolving digital landscape.