*Page 2161 - 2172* **DOI:** *https://doij.org/10.10000/IJLMH.116949*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 7 | Issue 1**

**2024**

# Right to Privacy and E-Commerce: Legal Analysis

TIMNA BRIJIT TENNISON[1], RESHMA R.[2] AND SEENATH P. S.[3]

**ABSTRACT**

*Today, the world is moving towards e-commerce application in completing their daily jobs. An ecommerce application becomes the preferred medium to complete the day's tasks. The potential for wide-ranging surveillance of all cyber activities presents a serious threat to information privacy. It gives more bad results in personal information privacy. In any e-commerce activities, all personal information should be controlled including their disclosure in order to protect its privacy.*

***Keywords:*** *E - commere : Electronic Commerce ; CGST Act : The Central Goods and Services Act.*

## I. INTRODUCTION

In this digital world, e-commerce (electronic commerce) is crucial. The internet and technology have made e-commerce an essential component of international business operations. Customers and businesses have benefited from e-simplicity commerce's and advantages, but concerns over data security and privacy have also grown. The Indian court has upheld the constitutional right to privacy in online transactions. The Indian e-commerce market has grown exponentially in the last few years. Online business setup and operation are encouraged by a number of government initiatives, including Start-up India, Made in India, Digital India, Innovation India, and Skill India. As a result, the Indian e-commerce market is expanding at the fastest rate in the world - 51 percent annually.

The Central Goods and Services Act, 2017 defines "e-commerce" as "the supply of goods or services or both, including digital products over digital or electronic networks" in Section 2(44). Electronic commerce, or e-commerce, is the exchange of money or data via an electronic network, usually the internet, for the purchase and sale of goods and services. These commercial exchanges can be business-to-business (B2B), business-to-consumer (B2C), consumer-to-business, or business-to-consumer. The CGST Act of 2017 defines electronic commerce in

[1] Author is a LL.M. student at CSI College For Legal Studies, Kottayam, India.
[2] Author is a LL.M. student at CSI College For Legal Studies, Kottayam, India.
[3] Author is a LL.M. student at CSI College For Legal Studies, Kottayam, India.

 [ISSN 2581-5369]

Section 2(44).

Without gathering personal data from its users, an e-commerce platform can hardly function as a transaction processor. These platforms may gather direct information on their users, such their identity and financial details, or indirect information about them, like their purchasing habits and personal preferences. Due diligence must be taken to ensure that this information is used appropriately and stays out of the wrong hands when it is obtained. Cyber theft and other criminal activities can also target the data that an e-commerce website gathers and stores. The e-commerce website has an obligation to take appropriate action to stop the same from happening in the future.

- In India, the right to privacy is not explicitly mentioned in the Indian Constitution but it is recognized as a part of the Article 21 of the Constitution.
- Privacy protects private data, communications, and space. the Puttaswamy case states that Privacy encompasses the right to keep personal information private, make decisions without interference, and regulate personal information distribution. it includes Data privacy.
- The right to privacy is a fundamental human right that is recognized in various international and domestic laws.

### (A) What is Privacy?

Privacy generally is central to our dignity and our basic human rights. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis, in[4] who defined privacy as: "the right to be let alone" Besides that, there are a number of privacy definitions. From the information system views, privacy is a right of individual to determine for themselves when, how, and to what extent the information will be released[5]. Goldberg defines privacy as an ability to control collection, retention and distribution of themselves[6]. The definition of privacy according to Ross Anderson is "the ability and/or right to protect our personal secrets, the ability and/or right to prevent invading our personal space[7]" Privacy is held to be valuable for many reasons. Most often, it is held to be important because it is believed to protect individuals from all kinds of external threats, such as defamation, ridicule, harassment,

[4] S. Warren, L. Brandeis, The Right to Privacy, Harvard Law Review 4, pp. 193-220, 1890.
[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic databases. In The 28th International Conference on Very Large Databases (VLDB), 2002.
[6] Goldberg, I., Wagner, D., Brewer, E., Privacy-Enhancing Technologies for the Internet. Proceedings, IEEE COMPCON '97, 1997, 103-109.
[7] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed System. Wiley Computer Publishing. New York, 2001 612 pp.

 [ISSN 2581-5369]

manipulation, blackmail, theft, subordination, and exclusion. It has also been argued that privacy is a necessary condition for autonomy. It is because without privacy, people could not experiment in life and develop their own personality and thoughts, because they would constantly be subjected to the judgment of others. From the information system views, information privacy can protect individuals from misuse of data, or unauthorized access to, or modification of information could adversely affect, or be of risk to the owner of that information. An important principle used in privacy protection in Western nations is that of informed consent: it is often held that citizens should be informed about how organizations plan to store, use or exchange their personal data, and that they should be asked for their consent. People can then voluntarily give up their privacy if they choose[8]. It is the willingness of consumers to share information over the Internet that allows the transaction to be completed and successful. It is the ability that concerns with the protection of information about individuals that is stored in a database.

### (B) What is Right to Privacy?

On August 24, 2017, the Supreme Court of India ruled in a landmark ruling that the right to privacy act is a fundamental right guaranteed by the Indian Constitution. There are significant ramifications for the Court's ruling, which maintains that this right derives from the basic right to life and liberty. In this post, we'll talk about the right to privacy and determine whether it truly is a fundamental right.

### (C) Right to Privacy: Historical Background

Due to several rulings over the past 60 years, India's right to privacy has changed. Over the years, opinions regarding whether or not the right to privacy is a fundamental right have divided due to inconsistencies from two early rulings. It is imperative to assess and construe constitutional provisions in a manner that guarantees their alignment with international human rights treaties that India has ratified. The court held that privacy is likewise a basic prerequisite for the meaningful exercise of other constitutional freedoms.

### (D) Cases that Cast Doubts on the Right to Privacy

Retired Justice K.S. Puttaswamy challenged the validity of Aadhaar in 2012, arguing that it violates people's right to privacy, and he filed a petition before the Supreme Court. The federal government contended during the proceedings that privacy ought not to be considered a fundamental right. Two early Supreme Court rulings—MP Sharma v. Satish Chandra in 1954

[8] S. Warren, L. Brandeis, The Right to Privacy, Harvard Law Review 4, pp. 193-220, 1890.

 [ISSN 2581-5369]

and Kharak Singh v. State of Uttar Pradesh in 1962—which found that privacy was not a basic right, served as the foundation for the government's opposition to the concept.

**(E) Privacy is commonly understood to be equivalent to the right to be left alone.**

"The right to privacy is a fundamental and inalienable right that attaches to the person and includes all information about that person and the actions that he or she takes," the Supreme Court declared in the historic case of K.S. Puttaswamy Vs. Union of India in 2017. As an essential component of the rights to life and personal liberty, as well as the freedoms guaranteed by Part III of the Constitution, Article 21 safeguards the right to privacy.

Under Article 12 of the 1948 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR), people are legally protected against "arbitrary interference" with their family, home, correspondence, honour, and reputation. India joined on 10 April 1979 as a signatory. The European Union also recognises respect for one's home and communications, as well as for one's private and family life. This is addressed by the Data Protection Directive, which outlines the acceptable handling and use of information in Europe.

**(F) Key Elements in Right to Privacy**

The key points of the judgement are summarized below.

a) Right to Privacy is a Fundamental Right

The Indian Constitution's Articles 14, 19, and 21 grant the right to privacy, the Supreme Court affirmed, making it a fundamental right that doesn't need to be mentioned explicitly. It is an inherent right that is connected to the freedoms of life and death. It is an intrinsic and fundamental right that is attached to an individual and encompasses all personal data and decisions made by that individual. It shields a person against being watched in their residences, on their travels, and on their personal preferences, relationships, and eating routines, among other things.

b) It is Not an Absolute Right; it is Subject to Reasonable Limitations.

The Supreme Court was cautious to emphasise that there would always be justifiable restrictions on the basic right to privacy. It was decided that in order to protect legitimate state interests, the state could restrict the right to privacy.

c) Other Incidental Implications

The court's decision on the primary matter may not have the only effects on topics connected to the right to privacy. Additionally, it has recognised the influence that non-state actors may have

 [ISSN 2581-5369]

on personal privacy, especially when it comes to digital information privacy. Despite the fact that fundamental rights are often only upheld against acts of the government, some experts worry that similar principles may also be applied to the private sector given the judge's expansive phrasing and the degree to which informational privacy has been discussed.

### (G) Government Steps to Protect Privacy

- The 2019 Personal Data Protection Bill Draft governs how commercial and public entities in India and abroad handle individuals' personal data. Processing is allowed if the person consents, if there is a medical emergency, or if the state is providing benefits.
- Committee headed by B. N. Srikrishna: The government established a committee of specialists on data protection, with Justice B. N. Srikrishna serving as its chairman. The committee turned in its report in July 2018.
- The Information Technology Act 2000 (IT Act) creates safeguards against specific computer system data breaches. Precautions are included to stop unauthorised access to computer systems and the data they hold.

## II. RESPONSIBILITIES OF E-COMMERCE WEBSITES UNDER INDIAN LAW

In the cases of People's Union of Civil Liberties v. Union of India (2003) 2 S.C.R. 1136, Kharak Singh v. State of U.P. (1964 SCR (1) 332), and K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, the Supreme Court of India recognised the “right to privacy” as a component of the “right to life and personal liberty”. India does not have any particular laws pertaining to the protection of personal information. However, the Information Technology Act of 2000 and the regulations enacted under it provide a framework for the same.

This case addressed trademark infringement and data privacy. The Delhi High Court ordered X to stop displaying sellers' contact details on its platform because it violated data privacy. It also ruled that privacy cannot be used to prevent civil suit disclosure. Even if it violates privacy, the court ordered disclosure of relevant information.[9]

In this case, X challenged the Y's order, citing concerns over the protection of confidential business information. The court upheld the Y's order and stated that the right to privacy cannot be used as a shield to prevent an investigation into anti-competitive practices.[10]

### (A) The Information Technology Act, 2000

[9] Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. (2020)
[10] Google v. Competition Commission of India (CCI) (2020)

 [ISSN 2581-5369]

The "Information Technology (Reasonable practises and procedure and sensitive personal data or information) Rules, 2011" (the "Data Protection Rules") contain the framework for data protection in India. Per the regulations, personal information is divided into two categories: Sensitive Personal Data or Information and Personal Information (PI) (SPDI). Information that allows a person to be identified is classified as PI, and information related to a person's sexual orientation, finances, medical history, biometrics, and passwords is classified as SPID. Corporate entities that handle, hold, or deal with customers' sensitive personal information (SPI) must adhere to specific compliance criteria set out under the Data Protection Rules. These requirements include –

- Setting up and following a privacy policy that is within the framework of the Data Protection Rules.
- The obtaining of consent from the person who provides their SPID to the e-commerce platform.
- Providing the customer with an 'opt – out' mechanism through which they can withdraw their consent.
- Maintenance of reasonable safety practices that prevent the misuse of the information.

Any organisation that neglects to maintain and apply security procedures will be held liable, according to Section 43A of the Information Technology Act, 2000 (the "Act"). In addition, section 72A of the Act stipulates that violating a customer's confidentiality and privacy may result in a two-year prison sentence, a fine of up to one lakh rupees, or both.

**(B) The Draft National e–Commerce Policy**

In 2019, the Indian government released the "Draft National E-Commerce Policy." Establishing a thorough technological and legal framework for the gathering and handling of sensitive personal data is the aim of this policy. It also establishes guidelines for the processing of personal data and offers some limitations on the transfer of data across national borders. The following requirements must be met by commercial organisations that process sensitive personal data in India and store it overseas:

- Such data is not to be made available to other businesses outside of India, with or without the consent of the customer;
- Such data is not to be made available to any third party outside India;
- Such data shall not be made available to a foreign government;

 [ISSN 2581-5369]

- Requests by Indian authorities to access such data shall be heeded to immediately; The above-mentioned restriction does not apply to –
- Data not collected in India;
- Business to business data collected as part of a contract of a commercial nature;
- Software and cloud computing services which have no community or personal implications; and
- MNCs moving data across borders where the data is not generated from users in India.

Despite the fact that this Policy is yet to be brought into force, it is advisable for e-commerce website to comply with the same as it is reasonable to expect this policy to be implemented in due course.

### (C) Restrictions

The right can only be restricted by state action that passes each of the three tests. In order for state action to be justified as necessary for a democratic society, it must meet three requirements: first, it must be authorised by law; second, it must be taking aim at a legitimate state objective; and third, it must be proportionate, meaning that it must be the least invasive option among those available to achieve the goals. Reading the right to privacy judgement PDF is essential if you want to understand this right clearly. A legal principle known as the right to privacy has been applied in a number of legal frameworks to restrict actions by the government and private sector that invade people's privacy. More than one hundred fifty national constitutions reference the right to privacy. There is currently debate over whether the right to privacy act and intelligence services' ability to access and examine nearly every aspect of a person's life can coexist.

## III. Personal Information

Information holds significance in all forms of transactions, be they online or offline. Information privacy is becoming an increasingly important topic to take into consideration as web-based information systems continue to proliferate. Users provide personal information in order to receive services, but businesses also require personal information in order to operate. How the data will be gathered, used, stored, and altered must be agreed upon by both parties. Consequently, an increasing amount of personal data will be gathered and handled digitally. When using any kind of information system, but particularly web-based information systems, the owner releases data through the system in order to complete a task. Then, this data will be

 [ISSN 2581-5369]

processed to become information; will be stored, reused and manipulated. This information will be kept in a database as a record or reused in the future. There are four types of data involved in processing[11] :

i. Personal data: any data that can be used to identify a person such as name, address, telephone number.

ii. Sensitive data: any data that disclose information about racial or ethnic origin, religious, philosophical or other belief, political opinions, membership of parties, as well as personal data disclosing health such as health history, race, etc.

iii. Identification data: personal data that permit the direct identification of the data subject such as DNA, identity card number, etc.

iv. Anonymous data: any data that cannot be associated to any identified or identifiable data subject such as gender, type of disease, etc.

From the above classification, the first three types of data can be considered as sensitive information. Sensitive information is information that requires protection due to risks that could result from its disclosure, alteration, or destruction. This sensitive information should be protected to ensure their privacy. Based on[12], the conceptualization of privacy is built on two distinct categories of privacy:

i) personal information privacy, and

ii) non-personal information privacy.

IITF Principles defines information privacy as an "individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed and used. From the definition, we can make a conclusion that, the central component of information privacy is the term personal information. IITF Principles define personal information as information identifiable to the individual. Al-Fedaghi identifies that personal information privacy involves acts on personal information. Typically, "personal information" is defined as information that is owned by a person, such as name, address, contacts and others. Heikkinen et. al.[13] defines personal information as any information that is related to the individual person. From the above classification, a conclusion can be made that not all data

[11] P. Guarda, N. Zannone, Towards the development of privacy-aware systems. Information Software Technology (2008).
[12] Al-Fedaghi, S. S. 2007. Anatomy of personal information processing: application to the EU privacy directive. Int. J. Liability and Scientific Enquiry, Vol 2. No's ½, pp129 – 138.
[13] Heikinen, K., Juha E., Pekka J., and Jari, P. Personalized View of personal information. WSEAS Transactions on Information Science and Applications, vol. 2, No. 4, 2004.

 [ISSN 2581-5369]

need to be kept confidential. It depends on the data owner himself. For instance, suppose Person A consistently receives emails soliciting sales from unidentified companies. She dislikes receiving web catalogues from unidentified companies. Therefore, it is better to treat her email address as private information. However, if Person B works as a salesperson, getting an online catalogue will help him close more deals. Thus, it is okay with him to provide his email address. The definition of private or personal information is a difficult topic. "Privacy raises diverse concerns at different levels and means different things to different individuals, even the scholars who study it." In an online setting, businesses utilise and reveal personal data that belongs to the data owner. To meet its needs, the organisation will gather, store, and process information. Only authorised users should receive access to any personal information, and only for a short period of time. For this reason, we precede the "Disclosing the personal information" phase with another phase called "Controlling the personal information."

### (A) Personal Information in E-Commerce Application

The definition and explanation of private information and its privacy are covered in the preceding section. This part will carry on the conversation of the problems and difficulties associated with protecting personal data in an online setting. Ensuring the security and privacy of the information disclosed by the owner is crucial. Confidentiality, integrity, and availability are the three prerequisites for data security, as was covered in the first part. The first and most crucial thing to think about is creating a system that can strike the right balance between private information availability, integrity, and confidentiality. The term "e-commerce" refers to the global network of computers, consumer gadgets, and communication networks that connects everyone. The revolution in our communication infrastructure in particular, the explosive growth of the internet has fundamentally transformed how we create, acquire, disseminate and use information[14]. Virtual and digital malls have made it possible to access and complete entertainment and purchasing tasks instantly. Sadly, e-commerce applications also bring forth fresh issues. Individuals are already worried about their privacy, particularly with relation to personal data that e-commerce apps acquire, use, and retain. For instance, every transaction in an e-commerce application is made using an auto-debit or credit card. Users must divulge personal information in order to finalise a purchase. However, this kind of material ought to be treated as confidential and only disclosed to the extent necessary to achieve the stated goals. Only the owner should have access to personal information. However, in web apps, this data must be provided in order to complete the transaction. Even if private information is shared, it

[14] NETWORK WIZARDS, Internet Domain Survey, January 1997 (visited October 11, 2008) http://www.nw.com/zone/WWW/report.html

 [ISSN 2581-5369]

is typically done so for security and privacy purposes so that unwanted users cannot access it. For this reason, there are three main issues that need to be considered:

i) personal information should not be accessed by unauthorized users,

ii) only required personal information will be posed,

iii) personal information cannot be passed to those who do not need the information.

From a privacy standpoint, the most important aspect of cyberactivity is the vast amount of personal data it generates. A user uses her computer and the Internet connection to log into the Internet service provider she has requested from the comforts of her home. She chose to purchase a book from an online book retailer after looking through a number of retailers. She must give out her credit card number and other personal data, such her name, phone number, billing address, etc., in order to finish the transaction. In addition, the retailer's website can ask for her interests so that they can get in touch with their clients and tell them about new books that are available. This transaction involves three different kinds of transaction parties: the individual, the merchant, and the payment processor. The people give the merchant the information that is needed. Consequently, every piece of information that shows up on a user's credit card and shipping order is accessible to the seller. However, this information should only be accessed by authorised users for a brief period of time and only if it is necessary to fulfil the goal in order to preserve privacy and protect personal information. In this instance, the individual overseeing the transaction should have access to it, and the data may only be retained for a period of two weeks. The credit card company, acting as the payment provider in this instance, will gather subscription data, including transactional data, to be included on monthly billing statements. This data will include the merchant's name, city and state, date of purchase, and purchase amount. The cardholder's information, including credit worthiness, credit status, and credit capability—information that might be required by other credit card companies, insurance, or other justifiable business requirements—must likewise be kept confidential by this payment processor.

## IV. HOW E-COMMERCE VIOLATES RIGHT TO PRIVACY?

- Gathering and applying personal data
- Sharing of personal data by other parties
- Lack of data security measures
- Inadequate privacy policies

- Need a balance between privacy and commerce
- Tracking and profiling of clients
- Data breaches
- Lack of regulation

**(A) Compliance requirements if data of citizens of the EU is being processed**

The General Data Protection Regulations (GDPR) are applicable to Indian E- commerce entities if the following criteria are met –

- Presence in a country of the European Union;
- Processes data in a country of the European Union; and
- Processes/stores personal data of European residents

By requiring businesses to abide by the principles of protection from unlawful data processing, fairness and transparency, data integrity, and accountability, the GDPR sets a higher standard of data protection than Indian law.

**(B) Suitable steps that can be taken to protect personal data of customers from cyber theft.**

- Installation of a SLL certificate – This will guarantee that any data that is transferred encrypted from the customer's browser to the payment processing website. By doing this, hackers may be deterred from stealing confidential payment data as it is being transmitted.
- Web Application Firewall – A firewall can stop malevolent hackers from trying to access your server's resources. You can use your firewall to prevent incoming traffic from foreign nations if you would prefer to conduct business exclusively in India.
- Updating plug – ins – keeping you plug – ins updated will ensure that cyber criminals cannot hack their way in.
- Using automated anti malware software – By regularly checking the files on your website, you can make sure that the sensitive personal information you save there is protected all around.
- Backing up and restoring important data – This will guarantee that you can always go back to a previous version of your website that still has your clients' personal information on it in the event of a security breach.

 [ISSN 2581-5369]

- Being transparent in marketing – This will educate your clients about the intended use of their information. In the long term, this will benefit your business by forging a relationship with your customers. By following the aforementioned procedures, you can guarantee that your e-commerce platform complies with all legal standards while also gaining the trust of your customers.

**(C) Measures to be taken**

- Implementing secure data storage and transmission protocols.
- Limiting the collection of unnecessary personal data.
- Providing customers with options to control their data.
- E-commerce companies should be transparent about the usage and collection.
- The government should strengthen e-commerce laws to protect privacy.
- Establish a balance between privacy and e-commerce.

## V. CONCLUSION

One essential human right that needs to be upheld in e-commerce is the right to privacy. Without the individual's consent, personal data can be gathered, retained, or used in ways that may violate their right. Serious repercussions may result from this for people, companies, and society at large. Businesses must take precautions to safeguard consumer privacy and acquire express authorization before collecting and processing personal data in order to avoid these infractions. The right to privacy in the context of e-commerce can only then be completely protected. The transition from offline to online systems is a new trend in today's globe. It's critical to safeguard private data from unforeseen events. One potential answer for data security is data privacy. A balance between confidentiality, integrity, and availability is the foundation of both data security and privacy. Maintaining privacy means having a strong system that satisfies these three criteria in addition to safeguarding personal data.

*****

 [ISSN 2581-5369]