Data Leak- A Potential Challenge For E-Commerce Platform

Rushikanta Dash[1]*, Prof. Damodar Hakke[2]

***Corresponding Author: -** Rushikanta Dash

[1] Student, Symbiosis International (Deemed University), Symbiosis Law School, Pune, rishikant0671@gmail.com

[2]Professor, Symbiosis International (Deemed University), Symbiosis Law School, Pune, Symbiosis Law School, Pune, damodar.hake@symlaw.ac.in

Abstract

Modern consumer behaviour and technological advancements have replaced the traditional consumer buying and selling practices with online shopping, which makes it easier for customers to shop while lounging in their own space, place orders online, and then have their chosen products delivered to their addresses. With the increasing use of the internet and improved network systems, the volume of e-commerce transactions has increased significantly. Large-scale personal data collection and processing are now an essential component of the modern economy. Businesses can benefit from personal data and strong data analytics since they can supply incredibly specific information about customer preferences and behaviour. In this case, the value of consumer privacy in e-commerce cannot be overstated. Individuals' freedom and choices over their lives are related to their privacy, which should be protected from outside interference. The privacy risks related to consumer data in e-commerce have been examined in this study. The study aims to shed light on some of the methods used to gather data, situations in which they have been misused, and how major nations' laws have responded to these issues. Since internet follows no boundaries then it will be a great challenge for governments to deal with crimes related to web. Regulations have been introduced into the Consumer Protection Act, 2019 in order to prevent malpractices, e-frauds, and other offenses in this area and establish who is responsible for such wrongdoings. The Consumer Protection (E-Commerce) Rules, 2020 are created for this reason in order to put the Act of 2019 into force.

Key Words- E-Commerce, Consumer, Privacy, Consumer Protection Act 2019, Data Protection

DOI Number: 10.14704/nq.2022.20.9.NQ440057 **Neuro Quantology 2022; 20(9):536-543**

Introduction

Right to privacy with data protection is the new need in contemporary world.

The revolution in the fields of technology has affected the society and social transformation never thought about the privacy via world web, so now data protection is the new challenge for the current world. With the mushrooming limitless technology data privacy is a real concern for the current internet users unlike their forefathers who abhorred it.

E-commerce is an universal term to sale, purchase, market & distribution of goods through E-networks or web. India showed a drastic growth in the sector at an international level, it was achieved due to such a large population of the country. E-commerce sector showed a revenue generation of about $39 billion in 2017 to $120 billion in 2020, growing at an annual rate of 51%, the highest in the world. This stupendous development of the web-based business area is predominantly because of the increment of smartphones and web users lately. The quantity of web users in India has expanded from 445.96 million of every 2017 to 665.31 million out of 2019 and is supposed to increment to 829 million of every 2021. (Indian E-

commerce Industry Report, India Brand Equity Foundation)

The rising number of smartphones has changed the era of information and technology, since it creates an easy access to for the people reach out to different parts of the world. The businesses use technologies to its optimum uses. Companies use technologies at its best to reach out to its customers, in this process they violate the right to privacy of the customers. Businesses may obtain a large amount of data or information about their potential customers and analyse it much more quickly and easily thanks to the internet and communication technology. In order to stay up with advancement and security in the internet age, particularly in the realm of e-commerce, India enacted the Information Technology Act in the year 2000, which has remained ineffective despite multiple changes, due to the dynamic growth of internet worldwide. Various software packages are being developed around the world for collecting and analysing consumer data or information. On the one hand, such a transformation aids businesses in customising their promotion of their products or services on the other hand; it has created numerous obstacles and issues in terms of customer privacy, security, and data in the e-commerce sector.

Due to the difficulties of online privacy and data protection, consumers' positions in e-commerce are vulnerable. (Gagandeep Kaur, Jurisprudence of E-Commerce and Consumer Protection in India) In light of the above concept and concern, this article will attempt to analyse the legal and regulatory issues of privacy and data protection in E-Commerce, as well as the revolutions brought about by the World Wide Web (WWW) in our society, with a particular focus on the harm the internet has caused to our legal and regulatory system due to its attitude of knowing "no boundaries."

Research Question

- How the consumers can be saved from different cybercrimes like data leak, frauds, etc. which generally happens in certain obscure E- Commerce platforms?

Research Objective

- To understand the loopholes of E-Commerce platforms behind data leak
- To examine the regulations made by the Government to tackle data leaks

Data Privacy

2017 was the year in which the famous case of Justice K. S. Puttaswamy vs. Union of India & Ors. ((2017) 10 SCC 1) on 24 August, 2017 established the need for the adoption of a single statue legislation for data protection in India. It says privacy is innate to right to life & liberty guaranteed by Article 21 of the Indian Constitution. Thus, Right to Privacy is a Fundamental Right. Through Puttuswamy judgement the Supreme Court of India said it is mere responsibility of the State to protect & safeguard the privacy to individual dignity.

Right to Life in a different and wide way that made the Right to Privacy fall within the ambit of the right to life (1978 AIR 597, 1978 SCR (2) 621). Consumers don't care as much about their information or data as long as they get anything in return (An Analysis of E-Commerce, Its Impact Issues Concerning the Rights of E-consumers," Indian Bar Review, 4 5(1) (2018). Increased human connection on a digital platform at a high pace has prepared the road for privacy protection, which is now a top priority. The generation which has large amounts of data on the internet makes it more prone to be misused, and the availability of large amounts of data on the internet also raises concerns about privacy infringement. As a result, there is a concern and a need for a comprehensive law that provides a set of meanings for the term Privacy.

Even a single visit by a consumer to an E-commerce platform allows E-traders collect and analyse a large amount of data or personal information about the consumer. Individuals' financial histories, medical details, sexual preferences, shopping patterns, families, and address details are all examples of personal information.

E-traders do, in fact, create a detailed profile of their customers based on their online activity. In certain cases some data are supplied by the users knowingly or unknowingly. Some sites collect

name, address, e-mail, credit card information, other basic information at the same time users may voluntarily supply personal information through threaded discussion messages, which are achieved on the site, also many e-commerce platforms compel customers to register before making an order for goods or services and customers must go through this registration process are needed to provide a tremendous amount of personal information or data e-traders can sell this data or information to third parties. The host server records information while their frequent visit to the site and it can transfer the data of browsing history/habits to the third party, that's why we see the ad banners frequently related to our searches on the E-commerce platforms. But, if we look closer, we can discover that visitors are giving information in two crucial ways: first, data automatically acquired by the site's server software, and second, data collected by third-party advertising through our site.

In today's world data is nothing but pack of information about a person's personal choices and breaching such data can be understood as stealing someone's belongings from his house. Data protection is need of the hour for protection of personal data and privacy of an individual, without which there will be infringement of right to privacy.

Despite being a signatory to the Universal Declaration of Human Rights (1948). The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations) and the International Covenant on Civil and Political Rights (1996), India currently lacks a well-established data privacy protection policy.

Breach of Privacy and Data leak Issues in Recent Years

Zoom Video Calling Services

During the pandemic whole world shifted from physical to online platforms. Many educational institutes, governmental offices, hospitals, Court proceedings, etc. performed its meetings on online platforms. Zoom video calling application was most popular online platform during the lockdowns. The company used very weak TLS encryption for video calls, which should have been banned by the country's telecommunication laws. It was claimed that Chinese servers encrypted the servers despite the fact that the servers existed in India. However, India, which accounted for about 18% (The Future of Data Protection in India: A Case Study Analysis of Zoom) of all subscribers as of April 2020, handled the situation unexpectedly. On 6th February 2020, and 30th March 2020, the Computer Emergency Response Team of India (CERT-In) (CERT is a national agency which deals with computer security incidents.) published two advisories highlighting potential hazards related to the application. So, all governmental organizations secluded themselves from organizing any meetings on Zoom, but surprisingly no legal action was taken.

Unacademy Suffers Data breach

Unacademy is India's one of the leading online learning platform. Many students enrol on this platform to boost their preparation for competitive exams. This site collects a lot of "personal data" of students, such as name, age, email-id, phone number, credit/debit card details and other personal information. Unacademy platform got hacked and reports say that all "personal data" of nearly ten million students got leaked. To this the Co-Founder of Unacademy, Mr. Hemesh Singh confirmed about the breach but denied any leak of sensitive data like financial records. However a site named Bleeping computers who deals with computer security confirmed that the all the basic information as well as sensitive information has been compromised and it can be used against the concerned students.

As per Section 70-72 of Information & Technology Act, 2000 covers unauthorized access to protected system and breach of confidentiality. For such crimes there is imprisonment for up to 10 years with fine for such breach. (Riddhi Kaushik, Cyber Crimes in India - Trends and Challenges, 21 Supremo Amicus [224] (2020))

Domino's Data Leak

Domino's use phone numbers, address, credit card numbers, etc. to reach out to its customers with food. It maintains a database of the customers who order from its application or websites. On 16th April, 2021 an Israel based cyber-crime intelligence firm named Hudson Rock claimed that a group of hackers have taken the responsibility of hacking into Domino's data base and having 13TB of data about Domino's customers. They demanded Rs.40 million from Domino's or else the data will be leaked into the Dark Web.

Later on this data was leaked, to which Domino's released a casual statement that "no financial information of any customer has been leaked". No attention was given to this matter and no legal actions were taken.

WhatsApp's Privacy Policy

WhatsApp a social messaging application, quite famous among the people of India, made certain amendments to its Privacy Policies in 2021. These changes were exclusively for its Indian Customers. As per its new privacy policy it allowed Facebook to share customer's data in order to serve tailored advertisements. Given WhatsApp's clout in the Indian market, it refused to make any concessions, instead stating that consumers may either accept or reject the service. Finally, the only action that appears to have been taken is that of the Indian Competition Commission, which ruled WhatsApp's policy change to be arbitrary and ordered a comprehensive inquiry as of March 24, 2021.

How E-commerce platforms compromise Right to Privacy

Unauthorized Access and Hacking

Unauthorized Access in simple term refers to illegal access to the individual's computer system without their approval. In technical term it is trespassing on private property without their consent to retrieve files or data which leads to breach of privacy. It's also known as software manipulation. Sometimes it takes the form of hacking (Riddhi Kaushik, Cyber Crimes in India - Trends and Challenges, 21 Supremo Amicus [224] (2020)) which is unauthorized use of data to harm the network or obstruct the data flow.

Hacking is done for a variety of reasons ranging from personal advantage to monetary gain, including money theft and credit card information. Section 66 (Computer related offences) of the Information Technology Act of 2000 covers this offence.

Web Hijacking

It's one of the most discussed topics on cyber-crimes that is web hijacking. It occurs through software when the browser alters the activity of the browser. Some random person can use your window to search for information & can use it against the user. Now a day these technologies are used by the E-Commerce platforms without permission of the users. They use it to steal personal details from users to spy on users, to display advertisements related to user's searches, etc.

The hacker in certain cases may alter the layout of the web page, the home page, display an error page, or even deploy his own search engine in such an action. Section 420 of the Indian Penal Code applies to this offence.

Ransomware

In the digital age, when all information is saved digitally, information may be accessed twenty-four hours a day, seven days a week, via the internet, and readily retrieved at a lower cost. Due to cheap cost of internet and easy access to internet to every individual lead to Many thefts or cyber-attacks like spyware, malware, Trojan, phishing, intruders, spam, virus occurs. Ransomware is also a data theft. It is a kind of disease that if transmitted, it's difficult to get out. It infects all essential data and file in user's computer system. When ransomware affects the data then you are compelled to give ransom to the hacker to revive your data. And there is no guarantee that your data will be revived.

The Wannacry ransomware outbreak in 2017 was one of the most massive attacks ever seen. According to the 2017 e-Scan antivirus reports, India was one of the countries most impacted by cyber-attacks. Surprisingly, Madhya Pradesh was the worst-affected state in the country, accounting for 32.63 % of all ransomware assaults recorded, followed by Maharashtra

(18.84%) and Delhi (8.76%). FedEx, Nissan, German train firms, Russian railways, the Interior Ministry, communications providers including mega for Telefonica in Spain, and at least 16 NHS organisations in the United Kingdom were all severely impacted. Malware infiltrated some systems (Lawrence J. Trautman & Peter C. Ormerod, Wannacry, Ransomware, and the Emerging Threat to Corporations, 86 TENN. L. REV. 503 (2019).

Wannacry encrypts all user data and leaves only two files for the user to instruct on what to do next. Bitcoin is the currency of choice for hackers. If not, the file will be erased without warning. (A brief study of Wannacry Threat: Ransomware Attack 2017).

Phishing

This is one of the easiest types of cybercrimes since there is no need for direct contact between the attacker and the target. In phishing attacker attempts to obtain user credentials such as passwords, credit card numbers, and bank account information. The victim is contacted via email or text messages in order to persuade them to provide personally identifying information. Sending bulk messages, mails, links, etc. to a target increases the chance of phishing.

Online Scams

Ad postal scams are the most popular type of online scam in India. There are commercials depict product offerings that appear to be too good but the quality will be compromised. There are many unrecognized sites from where customers order the product but once the money is paid then the site goes ghost and you cannot contact any of the executive of the company.

The sole purpose of internet scams is to fool clients into thinking they are purchasing a real product at an incredible price. These frauds can be carried out through advertisements displayed in your browser or when visiting specific websites, as well as through bulk emails and SMSs. When these adverts are clicked, they might disrupt the system and reveal sensitive information.

Spam fraud levels reduced to 68 % of global email traffic in 2012, according to a Symantec Intelligence analysis (Symantec, 2012). According to the same research, the number of cases reached an all-time high of 89 % in 2010.

Salient Features of Consumer Protection Act, 2019

- The meaning of "consumer" has been expanded by the Consumer Protection Act of 2019. A "consumer" is defined as a person who purchases products or engages in a service through an offline or online transaction, an electronic medium, direct sell, or multilevel marketing, according to section 2(7) of the Act. As a result, the new Act and other laws added e-commerce transaction disputes to area.
- The Act also expanded the financial jurisdiction of the State National Consumer Commission and each District. When the price of the goods or services paid does not exceed Rs.10, 000,000/-, the District Consumer Forum is authorized to hear complaints. Similarly, the State Commission to deal with cases below Rs.100, 000,000 and National Commission to deal with cases of value up to Rs.100, 000,000 respectively. (Section-35(1) & Section-38(6), Consumer Protection Act 2019)
- The New Act specified about unfair trade practice in its clauses that says any trader, merchant, or service provider that shares a customer's personal information without the customer's consent will be termed as unfair trade practice. (Section-2(47) of Consumer Protection Act 2019)
- The new Act gave customers another option, allowing them to register complaints electronically in addition to the more conventional method of physically submitting them to the District, State, or National Commission. The Act also stated that the Consumer Court might give technical assistance if the complaint sought to appear and conduct the hearing via video conferencing.
- Any manufacturer, trader, retailer, or seller as well as any endorser, advertiser, or publisher who ever makes any false or misleading advertisements will now be subject to further penalties under the New Act. The Central Consumer Protection Authority has the authority to penalize violators by issuing fines or issuing prohibition or discontinuance orders to traders, manufacturers, publishers, etc. who are found to have used such deceptive advertising.

The Consumer Protection E-Commerce Rules, 2020 have been created by the Central Government in accordance with the authority granted by section 101(1) of the Consumer Protection Act 2019. It covers all types of products and services that can be accessed through electronic and digital networks, including digital commodities. It lists all types of unfair practices that apply to various e-commerce business models. It also specifies the obligations and liabilities of every type of e-commerce entity. And if any e-commerce business violates the a fore mentioned standards, the Consumer Protection Authority, which was appointed under the Act, will take legal action against it in accordance with the Consumer Protection Act 2019's regulations

Personal Data Protection Bill, 2021

As India continues to make strides toward becoming a digitally driven nation, the subject of how citizens' personal data is managed is the need of the hour. India was travelling in a rudderless ship of data & privacy till Justice K.S. Puttaswamy v. Union of India sparked by the arbitrary mandating of Aadhar to avail services. To address all of the difficulties that a technologically driven nation can confront, the government is working hard to adopt dynamic laws, like as the Personal Data Protection Act, which can not only deal with current issues but also adapt to the changing technological landscape.

In the Indian legal setting, the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are the most prominent weapons for dealing with data processing issues. The measures of personal data protection are outlined in Section 43A of the IT Act of 2000. It only covers the corporate entities, therefore many government organizations that collect and process personal data are not covered under the section.

The "Data Principal" is a natural person whose data is being gathered, by legal people by the Act's protection. The person collecting and processing the data as a "data fiduciary," which can be a person, a firm, or even the government, giving it a significantly broader scope than the IT Act of 2000's section 43-A. The GDPR, on the other hand, adopts a more explicit approach to defining personal data, identifying criteria such as a person's name, identification number, location, physical, physiological, genetic, mental, economic, cultural, or social identity. There is another section of bill in which the data cannot be collected without the prior consent of “data Principle”, its defined under section 3(36), that is sensitive personal data. These are

- Financial data
- Health data
- Official identifier
- Sex life
- Sexual orientation
- Biometric data
- Genetic data
- Transgender status
- Intersex status
- Caste or tribe
- Religious or political belief or affiliation

While the data principle wants to collect the data he should tell the reason behind the collection of data and risks associated with it. Furthermore, the Bill continues to rely heavily on the consent-based paradigm, even though only a small percentage of the population uses EULAs to review the terms of the agreement. It has, however, embraced a more progressive "opt-in" consent-based model, in which data fiduciaries can only use data if the data subject agrees. The problem is that these fiduciaries will be judged to have obtained consent through lengthy privacy policies and terms of service, which most people will not read.

Data Protection in Different Countries

European Union Data Protection Laws

The set of data or “big data” are more vulnerable to security risks. So, EU is developing it’s technologies and constantly working on Information & Technology laws to deal with it. These rules are not only limited to GDPR (General Data Protection Regulation) but also from legislative instruments from EU as well as at national level.

The NIS (National Security Directive) is continuously fulfilling the demands relating to

privacy and cyber security. From the year 2014, developments for privacy, e-commerce & data security laws in Europe are constantly working on it. It's making amendments on the basis of judicial decisions with the guidance of advisory bodies and expecting laws to be intact in a long run. While both the European Parliament and the Council have taken major moves forward on the most important pieces of legislation in the approval process, the CFEU (Charter of Fundamental Rights of European Union) mandated interplay between the two institutions has been fairly complicated.

As a result, the ultimate enactment has been delayed. (Consolidated Version of the Treaty on the Functioning of the European Union, art. 294, May 9, 2008, 2008 O.J. (C 115) 47)

Developments in Russia

The Federal Law on Personal Data No. 152-FZ, enacted on July 27, 2006, established the foundation for data protection laws in Russia (Law 152-FZ - Federal Law of the Russian Federation on Personal Data). Russian law's on data protection is largely influenced from European Parliament but it operates with its own specific laws.

For E.g. - Law 152-FZ does not differentiate between "data controllers" & "data processor", it has a single term that is "data operators". Definition of "personal data" is quite wide under the Russian law. It describes it in more accurate way compared to other states. "Personal Data" includes financial status, educational qualification, profession, etc. along with the basic information like name, address, etc. It also gives advance level of protection to data concerning race, nationality, political opinions, religious sentiments, health status, sex life, etc.

Recent amendment to the law 152-FZ done on 1st September 2015, says data flowing out of jurisdiction or flowing cross border, it's the responsibility of the "data operators' to get proper clarification of data, check it thoroughly then only the data of the Russian citizens will be transferred abroad.

Data Protection in United States

In the United States, privacy, e-commerce, and data-security law is fast evolving, despite wide variation across states, ambivalence regarding federalization, and mounting legal challenges. Since the failure of the US-EU Safe Harbour programme, government and corporate leaders have been in turmoil, and a path forward remains shifty as of this writing in 2015.

California law was amended in 2015 to strengthen data privacy. One bill tightened breach notification requirements and expanded data-protection regulations to include organ-isations that "maintain," rather than just own or licence, personal data. Another law established a limited right of erasure, in this the content shared by a minor can be erased by the service provider with the request of the minor, but it has certain limitations.

While the private sector is faced with technical specifications for breach notifications, enhanced encryption standards, drone over flight restri-ctions, and privacy protection for automatically harvested licence plate numbers and smart-TV voice recordings, the public sector is faced with a variety of challenges. The FTC (Federal Trade Commission) is quite active in dealing with cases regarding data protection. In the case of FTC vs. AT & T, FTC (FTC v. AT&T Mobility LLC, 87 F. Supp. 3d 1087 (N.D. Cal. 2015).) fined the giant company of $100 million for restricting mobile data traffic & the commission proceeded to battle the corporation in court.

FTC also won an enforcement action against the Wyndham hospitality (FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).) for business over stolen consumer credit data.

Conclusion

In today's world buyer-seller relation, E-commerce has become a vital part for. For such a high use of Online platform the central Government should find a proper uniform code with an amalgamation of Information & Technology Laws, Consumer Protection Law, as well as Competition Laws to overcome the breaches done by the e-commerce platforms while establishing a buyer seller relation. As we have discussed that there are current major flaws regarding safeguarding the consumer's rights and how India lacks the proper law to protect the rights of the customers compared to other major countries. Also the Government is

introducing new regulations or upgrading itself gradually to protect the rights of the customers. For example we can see there were many flaws in the Consumer Protection Act, 2019 but the Government introduced The Consumer Protection E-Commerce Rules, 2020 to terminate the breaches and confusions regarding the data protection of customers in the previous Act.

References

Neelam Chawla and Basanta Kumar, E-Commerce and Consumer Protection in India: The Emerging Trend (https://doi.org/10.1007/s10551-021-04884-3)

Akhil Surya, Analysis of the Data Protection Bill, 2021: Social Media Regulation andPowers of the Government, 2 Jus Corpus L.J. 241 (2021).

Aman Pandey & Hema Chaudhary, The Exigency to Address the Personal Data Issues: The Personal Data Protection Bill, 2019, 2 Jus Corpus L.J. 533 (2021).

Jasmien Cesar & Julien Debussche, Novel EU Legal Requirements in Big Data Security: Big Data - Big Security Headaches, 8 J. INTELL. PROP. INFO. TECH. &ELEC. COM. L. 79(2017).

Sambhavna Rai, Legal and Regulatory Issues of Privacy and Data Protection in E-Commerce and Social Transformation, 11 INDIAN J.L. & Just. 308 (2020).

Data protection in e-commerce

(https://www.ionos.com/digitalguide/websites/digital- law/data-protection-in-e-commerce/)

Why data protection is vital in e-commerce.
(https://www.freepressjournal.in/technology/why-data-protection-is-vital-in-e-commerce)