ARYAVART SHODH VIKAS PATRIKA
RNI TITLED NO. UPBIL04292
RNI REG. NO. UPBIL/2014/66218
PP. No.- 334-339
ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

Right To Privacy In Digital Age

DR. Ranbeer Singh

Assistant Professor, Faculty of Law, Agra College, Agra (Dr. B.R. Ambedkar University, Agra) (U.P.), India

Received-21.12.2023, Revised-25.12.2023, Accepted-30.12.2023 E-mail: aaryvart2013@gmail.com

Abstract: ***The humanity has benefited incredibly from mechanical headway. However, as technology advances, many of our liberties are currently at risk. As innovation propels, so does the right to security, which incorporates information that is continually gathered and handled in the commercial center. As a direct result of digitization, a number of illegal practices, such as data fraud, hoax contact, cyber harassment, and others, have emerged. Client's confidential information can much of the time be misused when it is provided to sites for computerized organizing, business, communication insight firms, state organizations, and others. There is no express regulation all through the country that administers the getting, filing, reconnaissance, recording, getting to, handling, dispersion, support, and so on. of information. This paper is an endeavor to concentrate on the issues including right to security and information examination in the computerized age. The issues surrounding privacy are examined from two distinct perspectives in this paper. The first chapter discusses the state's ability to spy on people. The second chapter acknowledges customers' concerns about their right to privacy being protected by the Competition Act of 2002 and concludes with ideas that can be derived from relevant international regulations and precedents.***

Key Words: : Cyber harassment, right to privacy, data fraud and international, regulations, filing, reconnaissance.

The notion of a person's right to privacy has many facets. It alludes to the unique privilege of an internet user to manage the accumulation, storage, and dissemination of his identifiable data. Private data of an individual entails within its ambit identification information, hobbies, preferences, as well as data of others whom they're connected to, schooling, wellness, and finances are all examples of private data. Confidential information might possibly be inventively taken advantage of for various targets, for example, government observing and business benefit producing. In spite of the fact that Constitution of India doesn't explicitly perceive "Right to Protection" as a key right, yet the Zenith Legal Power chose it to be a basic right, in August 2017. Despite numerous administrative efforts, neither a data protection legislation nor an agency currently exists in India. However, India has made significant progress in respecting individual privacy..

In "M.P. Sharma v. Satish Chandra, the Supreme Court decided that the right to privacy is not guaranteed by the Indian Constitution. The bench was considering if a search order granted under Section 96(1) CrPC is in violation of Article 19(1)(f) of the constitution. The Apex Court's dissenting opinion in Kharak Singh v. State of Uttar Pradesh, warrants special attention since it recognised that the right to privacy as a fundamental right is protected by Article 21 and 19(1)(d) of the Indian Constitution. The U.P. Police Regulations' provisions for continuous surveillance were under consideration by the Court in the present case. The accused was charged with dacoity but eventually found not guilty. With the advent of time, the Apex Court ruled that the right to privacy included and protected issues pertaining to the families, the household, and other private affairs, and are subjected to "compelling state interest." While debating the question of telephone tapping, the Supreme Court expanded the right to privacy to embrace telecommunications and found that doing so constitutes a significant breach of one's rights. In addition, the Supreme Court recognised the demarcating line between physical and mental privacy". "According to the decision in Unique Identification Authority of India v. Central Bureau of Investigation, it is against the policy to share biometric data of an individual who has been assigned an Aadhaar number with any third entity in absence of express authorization".

In "K.S. Puttaswamy v. Union of India, where the Unique Identity Scheme was considered in relation to the privacy concern was delivered. Recognizing that there is no clear framework for privacy in the Constitution of India, the constitutional bench had to decide whether the right to privacy is guaranteed by the Constitution and, if so, where it stems from. This judgement distinguished itself from earlier precedents by making the unequivocal conclusion that the Indian Constitution protects privacy as a fundamental right. In the chapter that follows, a significant point of decision will be presented. Alongside, the bench while making several observations studied the essential nature of privacy, made a comparative analysis of privacy legislations from various jurisdictions and recognized the wide scope of data and its utilization by the state and business, nationwide. Before the recognition of "Right to Privacy" as a fundamental right under Article 21 of the Indian Constitution,

Corresponding Author / Joint Authors

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

Section 43-A and 72-A of the Information Technology Act were specific provisions guarding an individual's personal data, other than the Telegraph Act, 1885 which governed communication interception. The recently enacted, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposes requirements on companies who gathered information in order to secure private data".

FUNDAMENTAL RIGHT V. STATE INTERESTS- End-to-end encryption, often known as "E2E encryption," is the process of encrypting the communications transmitted by one system and decrypting the same on the unit obtaining the information in order to secure information in motion, or data that is presently being exchanged or conveyed across the web. This technique of encryption shields the information from external parties, even the network on which it is sent, and guarantees that it isn't tampered with during transfers. It also safeguards the information by generating a unique key at the time of encryption. Therefore, E2E encryption aids in protecting users' online data trails in the internet age when they are always connected to the internet.

Ruth Gavison's "limited access theory" may be the closest relevant theory for the modern era, given that the discussion over E2E encryption is tied to state officials' exposure to the information being transmitted by a user. It states that privacy is "related to our concern over our accessibility to others. The effects of a data breach are severe in the technology age, when each smartphone serve as a virtual journal of the owner's lives".

E2E encryption is becoming increasingly important in the work of people in anti- establishment or at-risk professions, such as investigative journalists, activists opposed to human rights abuses, leaders of civil society, and even marginalised groups who face persecution. Therefore, it may be said that E2E encryption fosters and preserves the right to free speech. One could argue that maintaining the E2E encryption system would amount to promoting and safeguarding this fundamental right. Every Indian citizen is guaranteed the right to peacefully assemble without the use of force by Article 19(1)(b). E2E encryption actively promotes and defends these rights by preventing communication interception by other parties and preventing potential surveillance as a result. Therefore, it is reasonable to draw the conclusion that the right to create associations will be at larger risk without E2E encryption. Iran is one country that has restricted freedom of association by forbidding encrypted communication tools. Law enforcements reduced the speed of encrypted channels of communication to just 5% of the average internet speed during the 2013 presidential elections out of fear of demonstrations. This made it extremely difficult for the protestors to plan demonstrations. Similar to this, it is in the best interests of the nation to maintain a reinforced E2E encryption regime in OTT Communication in a democratic nation like India, where protests and public demands are an important part of the political process.

The reasonable limitations outlined in Article 19 serve as qualifications to the rights to freedom of speech and expression, the formation of groups, and peaceful protest. Even the right to privacy is not absolute and can be legitimately limited when it comes to nation's security and to further the interests of the state. The question is whether the justifiable limitations set forth in Article 19(2) are sufficient to limit or weaken the E2E encryption offered by OTT communication services. The Puttaswamy judgment's test, at best, provides an answer to this problem. "This ruling proposes a 'menu' of tests that could be applied to consider how the boundaries and application of the constitutional right to privacy might be decided in other situations. A law, a 'legitimate State interest', and the necessity of 'proportionality' are the three criteria the Court set forth to determine whether any State activity violates the basic right to privacy. The Court also reaffirmed the four sub-tests for determining proportionality of a state action that were adopted in a 2016 decision in Modern Dental College and Research Centre v. State of Madhya Pradesh. The state can interfere subjected to meeting the following criteria: (a) the goal must be legitimate (the legitimacy stage); (b) it must be a suitable means of achieving the goal; (c) there must be no less stringent but equally effective alternatives; and (d) the measure must not have a disproportionate effect on the right holder (balancing stage). Therefore, if state measures restricting the right to privacy fail the aforementioned conditions, they would constitute a fundamental right infringement".

The Information Technology (Amendment) Act of 2008 grants the Central Government the authority to create regulations for encryption over a digital channel in Section 84A. According to the clause, the state will have access to this authority in order to advance network security and e-governance. A preliminary proposal encryption strategy under this Section that the government issued in 2015 was strongly contested on two key grounds. First, for weakening the requirements for robust encryption, and second, for the government's complete disregard to the harm to user's right to privacy and freedom of speech. After that, the authorities revoked the guideline, and no new one has been released since then.

It would be reasonable to state that legal rights should be harmoniously construed with the broader public interest

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

and should not be allowed to interfere with preserving national security. A strict encryption policy that forbids E2E encryption from allowing the government access to any data, might potentially have an adverse effect on national security by preventing the State from taking action against terrorists by withholding the records of such individuals. That is the reason why India requested RIM's Blackberry to decrypt the data and share it on behalf of the terrorists responsible for the 26/11 terror acts. To improve the surveillance system and better identify any potential threats in India, the Indian government had sternly requested that RIM localise its data here. In a similar fashion, the Reserve Bank of India in April 2018 put out a circular requiring that all "data relating to payment systems" are "stored in a system only in India" within six months to mitigate any risk in banking or digital payment frauds.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 puts forward a significant incentive for OTT Communication platforms to comply them since, if they don't, then the "safe harbour" statute no longer applies to them. In essence, safe harbour law declares that platforms won't be held liable for user-posted content. Consequently, it may be said that the businesses are in a Catch-22 situation, meaning that either they adhere to the laws and severely weaken their encryption system, or they lose the protection of the safe harbour statute and may be held responsible for anything users publish on their platform. This demonstrates how crucial it is for the Government that the suggested modifications to the intermediary rules are implemented. One of the most significant changes that was brought from the IT Rules, 2011 is that the government now requires intermediaries, such as OTT communications platforms, to respond to data requests from "any government agency" within 72 hours after receiving Court orders. However, what type of information can be requested has not been limited, this is a hurdle again in protecting privacy of the users.

In 2018, "the Ministry of Home Affairs (MHA) issued an order authorising ten central agencies to intercept, monitor, and decrypt any information generated, transmitted, received or stored in any computer stating this is done with a view to safeguard national security. However, this clearly fails the test laid down by the Puttaswamy decision".

Using cutting-edge technology solutions, digital contact tracing is another method of state surveillance that aids in identifying and identifying those who have been in close vicinity to someone who has been identified and exposed to the dangerous Covid-19 Virus. These apps also assist in swiftly detecting other nearby individuals and provide instructions for taking precautions and medical assistance to stop the spread of infectious viruses. These apps mostly rely on Bluetooth and GPS, with a few apps using both technologies simultaneously. The "Bluetooth Handshake" is the process by which two devices that are passing close to one another create radio waves that are picked up as waves by the other device within a set time and distance. A user's data is gathered by Contact Tracing Apps over a set period of time, and it is then processed and analysed over time on a central or decentralised server. Decentralized servers store user phone or Bluetooth device data locally on the individual device until and unless the user is tested positively or exhibits any symptoms, at which point the data is sent to the server and can be searched by other users who have come into contact with that positively diagnosed individual. Centralized servers store user phone or Bluetooth device data on a centralised server of the government.

India joined the Five Eyes Intelligence Alliance on October 11, 2020, and they jointly released a statement in which they essentially sought the installation of "backdoors" in the E2E encrypted systems used by the multinational IT corporations. According to Ex- USA President Obama, the back door should only be built if its advantages transcend its drawbacks. The author believes that the drawbacks of creating a backdoor would, however, exceed any potential gains. This is because, even while government officials might use the backdoor, it might also establish a weak scenario where hackers and international agents could take advantage of, resulting in widespread surveillance and a violation of the right to privacy.

A backdoor that may be abused was spotted in Greece in 2005; this incident is regarded as the "Athens Affair". At least 100 public officials' smartphones, particularly those of the Greek President and Prime Minister, were tapped as a result of the event. According to popular belief, the National Security Agency worked with the Greek law enforcement agency to oversee the 2004 Olympic games as a preventative measure against any prospective terrorist strike in the wake of the horrific 9/11 terrorist attacks in 2001. Conversely, the NSA, which was presumed to end the complete procedure after the Olympic games were a hit, proceeded mass surveillance on public authorities through Vodafone Greece, the largest cellular service provider in Greece. This also resulted in the potentially malicious demise of a techie working for Vodafone, Greece. As a result, it is clear how a backdoor may enable a foreign government to survey key leaders in any nation and violate their right to privacy.

DATA UNDER COMPETITION LAW- The traditional interaction among customers and enterprises is drastically changing as marketplaces increasingly function in a "digital economy." The phrase "digital economy" refers to markets where

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

computer - based technology assist the sale of products and services. Commercial strategies in this sector are centred on a flow of "information" among customers and companies, which is one of its defining characteristics. Customers' private data makes up a substantial portion of this data exchange. Customer information has in many respects evolved into the "currency" of this virtual marketplace. They can more efficiently offer their products and solutions thanks to the evaluation that results from the mining of sensitive information. They are now able to generate need by capitalising on customer behaviours and purchasing habits, thus they are no more dependent on the natural cycle of demand and supply. Two primary issues arise from the mining and processing of individual information by businesses: (a) the risk to customer privacy and rights, and (b) the widening gap across companies that are able and unable to extract customer information. Since the main objectives of antitrust law are economic efficiency, consumer protection, and competitor protection, the regulation of consumer data in this digital economy becomes a concern and is covered by antitrust laws. However, conventional competition investigation solely considers "price models." "Pricing models" are a variety of techniques used by businesses to set their prices for their products and services. Customer information is a "non-pricing model," hence it is not considered in the standard antitrust examination.

Amazon.com, Inc., the top e-commerce site, can be used as an illustration on how data privacy infractions can result in a decrease in customer wellbeing when seen through the perspective of competition investigation. Amazon used its data stored in 2000 to estimate the maximum DVD pricing American consumers might be capable of paying or were prepared to engage. This was known as the "Price Test." It gave a pioneering illustration of how virtual channels may enable first-degree pricing bias strategies using data collected, however it was ultimately scrapped as a result of public outrage. Such actions lessen customer satisfaction in an economy that is cutthroat. Akin to this, Uber Technologies, Inc. is aware of its customers' commute routines, which allows it to identify where they live, dine, exercise, etc.

Smart speakers that require certain "wake words" to operate, like Amazon Echo or Google Home, always have their surveillance feature on. It was reported that the firm Cambridge Analytica had reportedly mined data from 87 million Facebook accounts to conduct protest movements around the 2016 US Presidential Election, a controversy that grew to be called as the "Cambridge Analytica Scandal".

Companies can violate user privacy under the current data protection frameworks in India and other countries provided they declare it in their terms of service. These terms and conditions are frequently lengthy, unclear, or contradictory. As a result, users have little choice, rendering the false notion of "permission" under data privacy rules.

Along with customers, non-dominant industry participants deal with a variety of issues related to data collecting and mining. It is practically impossible for such businesses to start accumulating their information. Additionally, dominating corporations often analyse and mine consumer data in the form of "unique" and "non-replicable" data. Since only a few companies can access this special data, it raises antitrust issues. Authorities throughout the world worry that the requirement for a high amount or diversity of data may result in "entry barriers" for new entrants and small businesses who are unable to acquire or purchase access to the type of data that is available to established enterprises.

Acquisitions and mergers enhance the market leaders' power. Companies with a lot of data combine to become "data richer" and obtain additional data sets. As a result, larger, dominant companies gain a strategic edge over weaker, non-dominant ones which do not have the same information accessibility. Instances include the merging of Google and DoubleClick and Microsoft and LinkedIn. LinkedIn's user foundation could considerably increase as a result of its merger with Outlook.com, according to EC, which could have an adverse impact on market competitiveness.

Antitrust regulators evaluate the "harm v. benefit" of such combinations to determine whether or not to approve them. Authorities evaluate the benefits that the new entity would experience as a result of the new combination of various data sets that it would get. This research is conducted in light of the market's lack of competition.

Furthermore, the EC claims that it is not automatically an anti-competitive practise when dominant corporations refuse to give rivals access to such data. However, the rejection by the dominant corporation may be seen as an anti-competitive behaviour when the pertinent data is crucial for rivals. In such circumstances, the competitor must show that the in-question data is unique and that there are no other ways to obtain the data it seeks.

CONCLUSION- The Court examined the right to privacy at the appropriate time. In India, the use of electronic governance has begun. The public's excitement for IT-based processes is changing, as proven by the measurements on web associations. Keeping this in mind, a security ombudsman could be a practical way to make sure that the state doesn't use its position while parliament tries to pass clear rules to manage such a right. In the United Kingdom, where identical procedures are used, the Investigatory Powers Tribunal, a court, is in charge of limiting the state's surveillance authority and ensuring that

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

no one's right to privacy is violated. Furthermore, a lawful body could arrange an interaction for proof based decoding. In accordance with this strategy, the law enforcement agency must provide sufficient evidence in court to convince the courts that decryption is necessary.

The antitrust investigation in the European Union takes into account five competition-related factors in addition to pricing models: cost, creation, quality, decision, and development. The EU says that businesses frequently use customer data for their own purposes, which could lower the quality of the services customers receive. Antitrust regulations apply when such a decrease is achieved by a consolidation or stems from the maltreatment of a prevailing position. The EU relied on non-price characteristics in a number of mergers, including Microsoft-LinkedIn, Facebook-WhatsApp, and Microsoft-Skype. To safeguard shopper government assistance, the EU has likewise passed the Overall Information Assurance Guideline. The Personal Data Protection Bill, which was recently put on hold, was supposed to establish a Data Protection Authority with the responsibility of safeguarding individual interests by preventing the exploitation of personal data. Moreover, it specifies punishments for handling or moving individual information in contradiction of the Bill, as well concerning re-distinguishing proof of individual information without clients' arrangement, yet the equivalent was removed to carry the demonstration with additional changes.

India is maintaining the provisions that protect national security while moving toward a more user-friendly privacy regime. Several digital giants would choose India as their governing jurisdiction if the nation could model a more robust framework by drawing inspiration from other nations. India will be able to achieve its goal of becoming a five-trillion dollar economy thanks to this.

REFERENCES

1. K.S. Puttaswamy v. Union of India MANU/SC/0911/2017.
2. MANU/SC/0018/1954.
3. Section 96(1), The Code of Criminal Procedure, 1973.
4. Article 19(1)(f), The Constitution of India, 1950.
5. MANU/SC/0085/1962.
6. Article 21, The Constitution of India, 1950.
7. Article 19(1)(d), The Constitution of India, 1950.
8. Govind v. State of Madhya Pradesh, MANU/SC/0119/1975.
9. People's Union for Civil Liberties v. Union of India MANU/SC/0149/1997.
10. Selvi v. State of Karnataka, MANU/SC/0325/2010.
11. MANU/SC/0374/2017.
12. Supra Note 1.
13. Article 21, The Constitution of India, 1950.
14. Section 43-A and 72-A, The Information Technology Act,2000.
15. Section 5 & 24, The Telegraph Act, 1885
16. Replaced Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Rules), 2011.
17. M. S. Panicker, "Contours of Right to Privacy in the Information Age: Some Random Reflections on the Puttaswamy Judgment", 1 SML. L. REV.136 (2018).
18. R. Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale LJ 421, 523.
19. Riley v. California, 189 L Ed 2d 430 (2014).
20. D. Kye, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (2015), A/HRC/29/32.
21. Article 19(1)(b), The Constitution of India, 1950.
22. Supra Note 19.
23. M. Gupta and S. Jha "The Inclusion of Data Privacy in Antitrust Analysis", NLUJ Law Review 2020.
24. Article 19, The Constitution of India, 1950.
25. Article 19(2), The Constitution of India, 1950.
26. MANU/SC/0495/2016.

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- IV, Issues-30, YEAR- Oct.-Dec.-2023

27. A. Singh and U. Agarwal "Privacy, National Security, and Government Interests: The Many Facets of End- To-End Encryption in India" Journal on Communication, Media, Entertainment & Technology Law, 2021.
28. Section 84A, Information Technology (Amendment) Act, 2008.
29. A. Singh and A. Pathak "Data Privacy in Covid-19 World: Contact Tracing Application", RMNLU Law Review Journal, 2021.
30. RBI circular on Storage of Payment System Data dated 06.04.2018 available at: https:/ /rbi.org.in/Scripts/BS_ CircularIndex Display.aspx?Id=11244 last accessed on September 13, 2022.
31. Section 79, Information Technology Act, 2000.
32. Rule 3 (1)(j), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
33. Ministry of Home Affairs Order dated 20.12.2018 https://egazette.nic.in/WriteReadData/2018/194066.pdf
34. Issued by exercising power under Section 69(1), Information Technology Act, 2000.
35. India Joins Five Eyes, Japan in demanding backdoor into Whatsapp end to end encrypted chats, India Today, available at: https://www.indiatoday.in/technology/news/story/india-joins-five-eyes-japan-in-demanding- backdoor-into-whatsapp-end-to-end-encrypted-chats-1730681-2020-10-12 last accessed on: September 20, 2022.
36. Remarks by President Obama and Mrs. Obama in Town Hall with Youth of Northern Ireland, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/remarks-president-obama-and-mrs-obama-town-hall-youth-northern-ireland last accessed on: September 20, 2022.
37. Adam C. Uzialko, How Businesses Are Collecting Data (And What They're Doing With It), available at: https://www.businessnewsdaily.com/10625-businessescollecting-data.html last accessed on September 11, 2022.
38. Peter Swire & Lagos Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L. Rev. 335 (2012).
39. Ben Dickson, Beware the privacy and security risks of smart speakers, TechTalks (June 5, 2018), https://bdtechtalks.com/2018/06/05/google-home-amazon-echo-privacy-security-risks/
40. Marc Israel, The CMA launches a new market study in a bid to keep pace with afast-moving digital economy, White & Case (July 9, 2019), available at: https://www.whitecase.com/publications/alert/cma-launches-new- market-study-bid-keep-pace%20fast-moving-digital-economy last accessed on: September 13, 2022.
41. Charmy Harikrishnan, Micro targeting of voters can swing entire elections: Bartlett, who discovered Congress poster in Cambridge Analytica office, Economic Times, available at: https://economictimes.indiatimes.com/news/politics-and-nation/micro-targeting-of-voters-can-swing-entire- elections-bartlett-who-tweeted-congress-ca-poster-pic/articleshow/63659215.cms last accessed on: September 13, 2022.
42. Press Release, Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions (Dec. 6, 2016) (on file with European Commission), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284.
43. Case COMP/M.7217, Facebook v. WhatsApp, EUR. COMM'N (Oct. 10,

*****