



DECODING THE TECHNOLOGICAL PARADOX: THE CROSSROAD BETWEEN TECHNOLOGY AND PRIVACY

Maanya Jain * & Aastik Suryavanshi**

Abstract

With the advent of modernization and introduction of technological advances in India and abroad, we have seen that there has been an invasion of privacy which is a fundamental right under Article 21 and even as a human right. Privacy is now a universally acknowledged phenomenon and has been recognized by various countries worldwide. For instance, Americans have cared a lot for installing privacy as a generic routine in their lives in the digital landscape which is parallel to human arena. The computers have wholly taken control over human lives. Technology has advanced itself so high that now whatever we search on any search engine or maybe how we feel or think is been "heard" by the phones, computer or any gadgets which are technologically advanced. Thereby, we get recommendations about similar things. Isn't this an invasion of privacy? Humans have absorbed technology quite well that they do not know the implications as well as they do not even realize that their privacy has been hindered. Thus, there exists a paradox. The article dives deep into how technological advances with the advent of modernity and global rise in adding of technological gadgets has invaded individual's privacy.

Keywords: Privacy, technology, data protection, technology illusion.

* Student, B.A. LL.B. 4th Semester, Vivekananda Institute of Professional Studies, New Delhi. Email id- jainmaanya03@gmail.com, Contact No.-8826032699

** Student, B.A. LL.B. 2nd Semester, National Forensic Science University, Gandhinagar, Gujarat. Email id- aastiksurya86@gmail.com, Contact No.-9999081429

I Introduction

A STATE is built because of its citizens. Human life and its holiness are inviolable for any state and it thereby puts up an obligation on the state to fulfill the needs and care for its people. People are required to have certain guaranteed rights such as human rights and fundamental rights as given extensively by the Constitution of India. Ever since the 1990s, when computers advanced in human life there has been a need to keep a check, an eye on technological advancements so they do not hinder or outright the other rights of humans. The Constitution of India has developed itself by various inclusions of rights under Article 21. Article 21 of the constitution states as-

Protection of life and personal liberty

No person shall be deprived of his life or personal liberty except according to procedure established by law.¹

This article has been widely used and its scope has been expanded to everything that is required or protects the human life and liberty. It is one of the most interpreted Article of the Constitution as well. Under Article 21, the idea of privacy was first added in the case of *M.P Sharma V Satish Chandra*². The case is one of the significant one because it questioned whether privacy is an explicit fundamental right under the Indian Constitution. The question was also raised that whether searching of documents amounts to violation of privacy. The court held that privacy is not a fundamental right mentioned in the Indian constitution. In the

¹ The Constitution of India, art. 14.

² *M.P Sharma v. Satish Chandra*, AIR 1954 SC 300.

current scenario, it has become impossible to walk without technology in one's hand. Overall, it has taken over individuals' whole life.

II Privacy Lost: Technology Taking Toll over Humans

The parallel world of technology though very helpful but can be equally harmful for us. Privacy intrusion is quite prevalent nowadays. Privacy is difficult to define as it is an abstract concept. Privacy to sum up is defined as the state of being alone, not being under surveillance or in a state of being alone and not being watched by others. Technology has cherished itself as a long way to modernise the real world. It has taken toll over us. Privacy has left the idea with humans. Earlier, when people did not had access to such abstract of technology, they had freedom, they had privacy. Nowadays, privacy is no longer with us, our gadgets like our phones "hear" us. You may have noticed that whatever you feel or have searched on any search engine comes into your recommendations and feed as well. Take the case of Instagram, it shows the feed or even recommends as per your mood or your previous searches. Thus, it has become impossible to walk on this dual world without technology and that's why it has taken toll over us.

There are several cases such as data leak scams, easy access to your accounts, enabling of location access to all, sharing everything of ours on social handles and many more that unable technology to get into our lives. The recent film - CTRL shows that how a simple reliance on technologically advanced applications take control over us. They fulfil every requirement of ours from keeping reminders to calls and messages etc. The United States has taken major steps to protect data and human privacy and same in the case of India, the government has taken various

steps. For instance, data protection laws and various other ways to restrict the technology addiction.

In the case of the major nation- The United States, majority of the citizens feel that they are under surveillance and their data is being infringed by technology and the companies concerned. The data is used and sold for illicit purposes. Data driven service providers extract data from their consumers and there is a potential risk of that data being leaked. Also, there is a general lacking of this knowledge among people as well. People tend not to read those privacy rules or the terms and conditions listed at back and thereby they fall in these tactics.

III The Growth of Privacy: India

In India, the tapestry of privacy was not earlier an embedded idea under the Constitution, not explicitly or even under right to life and liberty under Article 21. The Indian legal history took itself a drastic question of whether privacy can be considered as a fundamental right or not. It was for the first time in the tapestry of India this question was raised in the case of *M.P Sharma v Satish Chandra*³, the answer of the Apex Court of India was in denial. It was held that privacy was not a part of any fundamental rights and checking of government related documents was not a part of privacy violation. This was the earlier time period of 1954 where the interpretation of the Constitution was exact point to what was quoted. For instance, the interpretation of Article 19 and 21 was not broad, it was narrowed down. However, with growth of time in the year 1964 in the landmark judgment of *Kharak Singh v State of Uttar*

³ *Supra* note 3.

Pradesh⁴, the court again did not recognise the importance of privacy as a fundamental right. However, Justice Subba Rao in his minority view jotted down the need to recognise the need of privacy in future amendments of Constitution. In the year 2004, PUCL v UOI⁵, where the court ruled and held that privacy is an obligation of state to be maintained in individual sphere.

The Puttaswamy Era: Beginning of Privacy

With the advent of 2017, Retd. Justice K.S Puttaswamy took a major step with the filing of a petition challenging the scheme of Aadhar; questioning the collection of biometric data for Aadhar card purposes. The question was raised that whether such collection of data is valid or not as per privacy being a human right but not a fundamental right. The Apex Court for the first time recognised the need for inclusion of privacy. It was through this landmark case the footsteps of privacy were placed in India. Later, with post Puttaswamy era, India introduced a set of Data Protection Laws to uphold data privacy from technology to its citizens.

IV The Introduction of Data Protection Laws: The Idea to Fight Technological Paradox

India is one of the most populous countries in the world, and to take cognizance of an individual's data and to protect it from the illusions of technology, the government took a step to introduce data protection rules. Every domain across the arc of globe is being digitalised and we are just a click away to get connected to anything at any time. Individuals

⁴ *Kharak Singh v. State of U.P.*, 1964 SCR (1) 332.

⁵ *PUCL v. Union of India*, (2004) 9 SCC 580.

have attached themselves to the realms of technology and thereby it thus required an urgent need for such laws.

What is Data Protection and the Need to Protect it?

Data is an abstract form of information that one holds. It may range from holding personal information to ethnicity of credentials. It is to understand the term data privacy means that what all information does a user or a consumer wants to share or communicate with third parties. It centres itself around an individual. The need of data protection is listed down –

1. Data is something that is considered to be the part of liberty. It is because data falls in the personal ambit and is totally on the discretion of individual to share what he/ she likes. There must exist a difference between personal and non- personal data.
2. Additionally, to build a trust among individuals and the concerned authorities that their data is safe, it is necessary that such an arena be regulated. Hence, laws dedicated to keep an eye on data infringement and privacy as well as to ensure a recourse for victimised individuals.
3. Data protection and the interconnection between the fundamental as well as human right: The Right to Privacy. It implies that every individual has the right to preserve their data. Privacy is an abstract idea; difficult to define. It was in the year 2017 the urgent need to recognise privacy as a fundamental right was recognised.

4. The major reason why we need data protection laws is because of the technological threat, the illusion of technology being our friend. Technology has hampered data privacy to a large extent. It is slowly taking toll over individual's lifestyle. The illusions of technology smartly gather individual's data and that may lead to data breaches and leaks.
5. Surveillance and children's privacy is of utmost importance. Children may fall into the traps of technological advances and thus, there comes a need to keep an eye and the need to regulate the same.

The Digital Personal Data Protection Act 2023

With gradual advances in technology and advances in gadgets, the nation felt the need for protection of their data. This has now been regulated through the digital personal data protection act 2023 which has been implied for protection of data available at government authorities, individuals. However, it does not include that data which is shared as per the consent of the person concerned or they, themselves have shared to it public at large.

Under section 2(t) of the act that defines personal data reads as,

*"Personal data" means any data about an individual who is identifiable by or in relation to such data;*⁶

This simply refers to that data that an individual holds at his or her level. This may include biometrics, credentials etc. Further, personal data is something which is related personally to the person concerned.

⁶ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 2(t).

Under section 2 (u), personal data breached is defined as-

*“Personal data breach” means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;*⁷

This definition includes that breach or misuse of personal data for illicit purposes that is done for wrongful gain or to exploit the latter.

Through the definitions it is clear that the act aims to reduce data breaches and to lessen the exploitation of data through various entities concerned as that creates a crossroad between privacy and technology and that is what we define it as a technological paradox or illusion. As learned individuals, we must understand how technology has overpowered humans and their information simply by keeping an eye on our actions. Thus, these rules in the DPDP Act aims to reduce the paradox existing between human privacy and technology. Cyber-crimes, cyber-attacks or ransomware attacks have increased in this sphere and thus requires such acts to regulate and solve the grievances of the people concerned.

V Right to be Forgotten in India and GDPR

Privacy has been held to be a fundamental right in India after the landmark judgment of Retd. Justice K.S Puttaswamy. It is to be noted that there is nowhere mentioned the ‘Right to be Forgotten’ also referred to as ‘Right to be Erased’ caught attention in the case of Sri Vasunathan v.

⁷ *Supra* note 6, s. 2(u).

The Registrar- General in the Hon'ble Karnataka High Court. The right to be forgotten is not a recognised fundamental right but is merely recognised as a privacy concern which was recognised by the European Unions' General Data Protection Regulation that existed back since 2018. The idea behind the right to be forgotten is that the data or information that is been held or is being stored by the concerned companies should be 'forgotten' or 'deleted' from online databases. This legal framework allows individual liberty to store his or her data and information wherever they like. It is also a necessary in criminal cases which are of grave nature such as rape, for instance, the name of the victim should ideally be forgotten or not to be exposed to the general public because of privacy concerns. Quoting the Delhi High Court judgment of Google LLC v. Vishaka Industries, the court raised a concern over defamatory content published.⁸ It asked the respondent to delete the content on certain webpages. This judgment analysed the need for the right to be forgotten. The significance of this right is that it upholds privacy, restores and protects the dignity of the individual, reduces risks of defamation as well as is a part of freedom and liberty.

GDPR, which is also called as General Data Protection Regulation was introduced by the European Union back in 2018 to provide for a systematic legal framework for rise in data leaks. It rests an obligation over the companies and organizations and imposes penalties against the ones who cause privacy violations. Through the introduction of GDPR, a stance has been taken up globally to ensure security standards.⁹

⁸ Priti Raj, Right to be Forgotten, *available at*: <https://www.clearias.com/right-to-be-forgotten/> (last visited on January 9, 2025).

⁹ Ben Woford, What is GDPR, the EU'S new data protection law, *available at*: <https://gdpr.eu/what-is-gdpr/> (last visited on January 9, 2025).

One of the most famous cases of Right to be forgotten in Europe and the non-compliance of GDPR is against Facebook. The case was filed by Max Schrems before the Irish data protection commissioner. The facts revolved not exactly regarding Right to be forgotten but rather 'right to be erased'. Mr. Max asked Facebook to send his data that was stored with Meta servers and thereby he received 1000 pages file which included all his information including the ones which he believed was deleted.¹⁰ Thus, he filed a complaint that his privacy had been overlooked, there has been shadow profiling and technology has illusioned him to believe that the data was deleted. The complaint mainly focused on that Facebook is not following the data policy of European Union and making data just invisible from the user's preview is not valid and simply an overshadow over privacy. Thus, consent is important. Based on the same facts was the Google case where the tech giant made certain links unviewable from public arena but it was still been stored in their databases.

VI The Crossroad between Privacy and Technology

Back in the year 2017 when privacy as an abstract idea was recognised, the government did not at that point plan to introduce an Act for data protection. However, with excess reliance on the illusions of technology, the DPDP Act came into existence in the year 2023. In today's digital era, our personal data {as defined under Section 2 (t)} is collected by various social media sites and various e-commerce platforms and later processed by various organizations. With rise in cases of such breaches,

¹⁰ Prashant Mali, "Privacy Law: The Right to be Forgotten in India" 7 *NLIU Law Review* 5 (2018).

it is necessary to safeguard the rights of people.¹¹ In the digital era, personal information has a golden value; it holds a lot of value nationally as well as internationally. Security of such personal information has been universalized. In the virtual world it is a matter of great concern. Almost every human activity transcends behind a footprint.¹² Innovation is a necessity since the society is dynamic in nature, but such an evolution should be taken in consideration of public trust and welfare. This creates a crossroad between privacy and technology; how both been essential to human liberty intersects each other. Privacy law has failed thereby to protect the individuals from observation.¹³ The major reason why the privacy laws are not enough to protect individuals from the illusions or paradox of technology is because they have not been implemented strictly. Adding on, people have violated these laws and there is no one to look after the violations. Citing a case is the Apple's Siri controversy where the law suit was filed against Apple's voice assistant Siri accused of recording and storing of voice commands.¹⁴ The question raised here was whether recording of voice commands without the consent of the owner is a violation of privacy. These invasions had begun in 2014 and continued till 2023 after which an outrage was seen among Apple users leading to a settlement to avoid potential risks. It is not just the case of voice assistants, rather with advent of new technology our 'voices' are heard by various other applications which potentially are the cause of

¹¹ Shruti Nair, How the DPDP Act protects your data: A guide to digital privacy rights in India *available at*: [https://www.parkerip.com / blog/ digital-privacy-rights-in-india/](https://www.parkerip.com/blog/digital-privacy-rights-in-india/) (last visited on 2 January 2025).

¹² Santosh Dalhich, Privacy in Digital age: The intersection of Technology and Law *available at*: <https://www.legalserviceindia.com/legal/legal/legal/article-17929-privacy-in-digital-age-the-intersection-of-technology-and-law.html> (last visited on 5 January, 2025).

¹³ Woodrow Hartzog & Evan Selinger, "Privacy Nicks: How the Law Normalizes Surveillance" 101 *Washington University Law Review* 717 (2024).

¹⁴ Kashish Saxena, Tech Privacy Cases: From Siri to Alexa, Are your conversations being recorded? *available at*: <https://www.businessworld.in/article/tech-privacy-crisis-> (last visited on February 9, 2025).

data leaks, hindering of privacy and a failure to the data protection laws. Even in India, there are various examples that depict the failure of the data protection laws and the non-compliance to such laws. For instance, the data leak case of Zomato back in the year 2016, where personal information of Zomato users got leaked that included email address and passwords of the users. The cases ignited the urgent need of cyber security and data protection measures. Not just companies but the government also faced a thrash when the biometric data of citizens got leaked due the Aadhar scheme. The apex court in this case mentioned the need for a proper legal framework to regulate the data sector in India and a set of regulations to deal with data protection and cyber-crimes which were at peak. In addition to these circumstances, the Reserve Bank of India had also guided the subordinate and commercial banks to look after the privacy of their customers and take measures to avoid data leaks.¹⁵ Thus, the technological paradox is at crossroad with privacy in modern day scenario.

Another instance where such a paradox exists is that where our 'voices' are been heard by our smartphones. Let's suppose, person A is with his friend, person B at his home where A intends to buy a smartphone that costs around Rs. 50,000. He expresses it and soon starts to see the recommendations of the smart phones that range from Rs. 50,000. This is what 'our voices been heard' means. Technology has reached to an extent where active listening by smartphones through artificial intelligence blended with technology is happening. Isn't this a privacy invasion? Yes. Our voice is a personal information that constitutes data.

¹⁵ Peeyush Raj Trivedi, Strengthening cyber security and data protection in India: available at: <https://www.legalbites.in/topics/articles/strengthening-cyber-security-and-data-> (last visited on: 8 January 2025).

Data invasion is happening every second, where what we feel, express is heard by our gadgets through active listening software. A study conducted by 404 Media reveals that big giants such Amazon, Google, Siri and various other voice assistants and Artificial intelligence tools collect the data.¹⁶ Recording of voices, collection of personal data such as email addresses and passwords are hinderance to privacy. This is where a crossroad occurs. A study conducted by Tidio concludes that 56 percent of U.S users suspect an activity that their phones are hearing them.¹⁷ The shady practices of giant tech companies to invade data privacy through the use of technology has hindered the fundamental as well as the human right of individuals.

VII Real-life Incidents and Case Laws

1. Meta and GDPR violations

Meta is one of the biggest giants in the technology sector which owns applications like Instagram and Facebook. The giant is accused of allegations against it that they have been using active listening software and has even faced heavy penalties due the same. Among the heaviest fines imposed is that of €1.2 billion when the parent company had transferred the data without user consent and without any safeguards.¹⁸

¹⁶ Nandini Yadav, "Is your phone listening to your conversations? Yes, and there is finally a proof: Story in 5 points" *India Today*, 6 September 2023.

¹⁷ Kazimierz Rajnerowicz, Is my phone listening to me? Truth or Myth, *available at*: <https://www.tidio.com/blog/is-my-phone-listening-to-me/> (last visited on 9 January 2024).

¹⁸ Kashish Saxena, Tech Privacy Cases: From Siri to Alexa, Are your conversations being recorded? *available at*: Tech Privacy Crisis: From Siri To Alexa, Are Your Conversations Being Recorded? - BW BusinessWorld (last visited on 9 January 2025).

2. AI training through breach of privacy- Microsoft

A study revealed that Microsoft has been using Skype and Cortana for training of their AI models. The voice they used to record used to contain sensitive information of the users and that was used to transliterate for AI. Later, Microsoft updated the measures and provided for stricter privacy norms.

3. The 2020 case of Unacademy

Inadequate privacy and security measures led to data leak and easy access to cyber-crimes of 22 million user data which included Gmail addresses, phone numbers and passwords, ultimately leading to the failure of data protection.¹⁹

4. Vidal Hall & Ors. V Google Inc

Vidal and 3 others filed a litigation claim on Google arguing that their personal information is being collected from a web browser called Safari. The claims were established through DPA (Section 13) where they believed their data was gathered. To invoke the DPA, they had to establish some pecuniary loss which did not occurred. However, the court took a view that it is not necessary to have pecuniary loss in such cases. Mere distress is enough to prove that there existed some scrutiny. The judgment has the following takeaways, there must not always occur some pecuniary loss, mere distress is enough to establish the infringement of privacy by the

¹⁹ Peeyush Raj Trivedi, Strengthening cyber security and data protection in India: An Analysis of Legal Frameworks and Case Studies, *available at*: Strengthening Cyber Security and Data Protection in India: An Analysis of Legal Frameworks and Case Studies (last visited on 9 January 2025).

respondent. Personal data also includes browser information. The DPA now also includes browser information as personal data. Any infringement of browser data is also data leak.²⁰

5. Google Spain v AEPD and Mario Costeja González

The case dealt with removal of personal information of a user from google in Spain. When he searched his name on google, there showed two publications on his name regarding confiscating of his house adding to it this news was also published in newspapers.²¹ The Spanish Data Protection Authority had dismissed the order stating that newspaper reports have been lawfully published and that data cannot be erased or forgotten. However, the publications made on google can be deleted. The search engines hold personal information that records in its indexing and it the legal right (as per GDPR) that such information shall be removed as per the consent of the individual.

VIII Suggestions

- Make active laws with regard to protection of privacy.
- Work proactively for complete implementation of the Digital Personal Data Protection Act 2023 in India and for clear guidelines for compliance and imposition of penalties for violations.

²⁰ Vidal Hall v Google: A new dawn for Data Protection Claims? *available at*: Vidal-Hall v Google: A new dawn for data protection claims? | Fieldfisher (last visited on 9 January 2025).

²¹ The case Google Spain v AEPD and Mario Costeja González of Court of Justice of European Union: A brief Critical Analysis, *available at*: The case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis – Homo Digitalis (last visited on 10 January 2025).

- Align India's data protection policies with global standards including the General Data Protection Regulation (GDPR) to enhance international cooperation and credibility.
- Boost awareness and digital literacy among individuals, launch campaigns to educate citizens on their rights under data protection laws and the risks of putting personal information online.
- Raise public awareness on the importance of privacy policies and terms and conditions, helping users in making responsible decisions related to their data.
- Enable measures to regulate big tech companies, put stringent regulations on tech companies regarding the collection, storage, and usage of their data with full transparency and accountability.
- Form independent regulatory institutions to monitor and audit tech companies with regard to their compliance with norms and privacy laws.
- Encouragement of Privacy Enhancing Technologies, promote the use of technologies that guarantee data privacy, including encryption, anonymization of data, and secure data sharing protocols.
- Invest in research and development of ethical AI systems that would intrinsically uphold user privacy.
- Creation of a Right to be Forgotten, formally recognize and implement the Right to be Forgotten in India such that individuals may apply for the removal of their data from online sites.
- Provide clear methodologies of exercising this Right with necessary safeguards not to conflict with the public interest or the right to free expression.

- Tighten cybersecurity provisions against data breaches along with ransomware attacks-especially with respect to critical areas like finance, healthcare, and governance.
- Mandatory requirement of regular security audits followed by penetration checking for organizations dealing with sensitive personal information.
- Promoting International Collaboration.
- Contribute to the ongoing global conversation on technology ethics vis-a-vis data privacy to regularize policies, share best practices.
- A concerted effort on the part of countries to prevent cybercrime from becoming international and for the humane treatment of data around the world.
- Promotion of Ethical Technology.
- Give the incentive to tech companies with user-centric goals in mind to radically transforms how a customer's journey with its technology works now.

IX Conclusion

There exists a paradox between privacy and technology where the rapid advancement of technology is at constant odds with the right to privacy. There is an expectation of borderline convenience and intrusion as technology become deep embedded within every aspect of human life. Legal creativity and careful implementation must also accompany the growth of technology so that liberty and dignity of an individual is not compromised. India has come a long way in achieving privacy as a fundamental right through various important judgements including Puttaswamy v. Union of India, which was a landmark judgement to aid in increasing protection against abuse of personal data and inducing trust.

Then the Digital Personal Data Protection Act 2023 is a step forward in preventing data abuse and addressing the unauthorized access of people's data. The most prominent concern remains to be whether these laws will prove effective or just be words on paper.

The noncompliance of the measures for personal data protection in various cases makes it necessary to have strong oversight from former regulators, if only so that technology companies such as Meta and Microsoft can be discouraged from such behaviour, and wider frameworks like the GDPR can be well effective.