



## DIGITAL TECHNOLOGY AND ITS INFLUENCE ON RIGHT TO PRIVACY

**Jennifer Akhtara Hussain**

*M.A, Cotton University*

*Department: Political Science*

Email id: [jennyakhtarahussain@gmail.com](mailto:jennyakhtarahussain@gmail.com)

### **Abstract:**

Human beings are thought of to be independent entities with an appetite for privacy and authority over particular parts of their lives. Everyone has an innate and inviolable desire for privacy, which is today acknowledged as a basic human right. Every individual's privacy must be preserved because it is an essential component of their existence and freedom. Researchers and legislators have occasionally acknowledged the importance of this basic right to privacy, and it currently occupies a unique role in contemporary life.

We are now living in the digital world. A fresh era with improved communication, quicker information exchange, and greater openness has emerged as a result of the development of internet technology and the expansion of its connectivity. But each thing has its advantages and disadvantages. Since the internet is being used more and more for the interchange of confidential, personal and business information, there also appears to be a spike in technological abuse, which is generally unavoidable.

Information exchange in the modern world has been made significantly easier by the revolution in digital technologies. Communications technology play a crucial role in everyone's life as well as the lives of all states, increasing the ability of businesses, authorities, and individuals to track down, capture, and acquire information. As a result, broad online tracking is not only possible but may even be encouraged by the technological foundations that underpin the world's governance, economy, and cultural affairs. This is because they lower the technical and monetary obstacles to detection.

Laws at the local and federal levels also protects the rights of all people to respect for their status, acknowledgement of their honour, and the right to family, home, and private affairs. Therefore, the fundamental significance and lasting value of the right to privacy and the obligation to ensure its respect are well understood both legally and in practise.

**Key words:** Technology, Privacy, Data

**Introduction:**

Technology and privacy are two interconnected ideas that need to be investigated and discussed together. By generating the ability to make and manage not merely material things but also pictures, social networks, and interactions between people, technology is an outgoing practise that symbolises the ability of societal systems to change them. Consequently, privacy depicts a crucial and sophisticated aspect of these interactions.

The idea of privacy is not new. Polis and Oikos, the general or civic sphere and the personal or domestic sphere, respectively, were the divisions of ancient Greece. On the other side, the right to privacy is an emerging idea. Though the right to privacy may encompass both physical privacy and privacy connected to interactions, the idea is today mainly about data security in light of media and the global web. The prospect of a global city, where the development of technology has united and connected the communities, economies and people of the globe, has become an achievable goal in the 20th century.

As stated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, nobody is to be a victim of willful interference with his or her family, home, or communications, nor shall he or she be subjected to abuses of dignity or character. Every person has a right to legal protection from these types of invasions or assaults. Other international documents, including human rights treaties, also contain related provisions.

According to Black's Law Dictionary, a person's right to stay by himself, the liberty of an individual from unjustified exposure as well as the liberty from unreasonable public intrusion into personal problems that are not inherently of public interest.

Mass monitoring methods are spreading across the globe, raising the risk that governmental authority over digital technology will be lost. In this view, only a small number of sophisticated nations have produced technology that makes it possible to obtain practically every bit of the World Wide Web's traffic, call records for individuals, computerised address books, and vast amounts of other digital data. Authorities could soon be losing their influence in this area, even though these acts are currently taking place with the approval of governments all over the world.

The Article 21 of the Indian Constitution states that No individual shall be denied the enjoyment of his life or personal liberty except in accordance with the procedure established by law. According to a broad analysis the right to life guaranteed by Article 21 encompasses beyond only animal survival or basic necessities of life. The right to privacy constitutes one of the many facets of life that provides an individual's existence with greater significance, achievement, as well as making life worthwhile.

For the very first time this subject had been raised in the matter of *Kharak Singh v. State of UP* in which the Supreme Court determined that Regulation 236 of the UP Police Regulation was unlawful because it conflicted with the provisions of Article 21 of the Constitution. The Court ruled that the right to privacy is a component of the right to safeguard the dignity of human life and individual freedom. In this case, the Court linked personal liberty and privacy. Particularly in the wake of domestic and multinational exchange of information tracking, online network surveillance, and the gathering of private information, international human rights law provides an apparent and comprehensive foundation for the advancement and safeguarding of the right to privacy.

### **Review of Literature:**

Luciano Floridi *Protection of Information and the Right to Privacy – A New Equilibrium?* talks about how the size and variety of communication is already amazing, the range and competence of harmful programmes pose an expanding danger and the type and extent of the sources have become possibly limitless. Nowadays, the quantity and varieties of both senders and recipients have increased rapidly, becoming practically limitless. Technology for monitoring is developed and used on an extensive basis by governments as well as corporations. The balance among freedom of expression, the freedom to access data, the right to confidentiality of data and data safety is being rebuilt by ICTs. With rising stress, novel disputes and possible conflicts inside this circle continue to develop. It appears that in this complicated circumstance, older legal as well as moral foundations could require to be strengthened and improved by innovative theoretical responses.

Daniel J. Solove *The Digital Person: Technology and Privacy in the Information Age* discusses how, in the context of the significant technical advancements, we need to comprehend and safeguard privacy. The old notions of privacy are inadequate. It also tries to challenge conventional ideas of privacy in order to address the effects of surviving in the

digital age. It talks about how digital technology makes it possible to maintain the details of our daily activities, including what we like and do not like, as well as who we are as individuals and what we possess. A digital assemblage that includes a large portion of an individual's existence, a lifetime documented in files and a digital individual assembled in global digital network is becoming more and more feasible. The author in the book also makes reference to "digital dossiers." A dossier is a compilation of specific information about a person. In order to gather evidence about an individual and make a decision, European courts employ dossiers. Dossiers, about every one of us have been generated today with the help of computers. Data is converted to decimal number format during the digitisation process, allowing computers to keep and process information with formerly uncommon efficiency

Lorna Stefanick *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World* highlights the significance of freedom of information and privacy (FoiP). It clarifies how FoiP supports effective governance, which is essential for a liberated, democratised, and financially prosperous country. It demonstrates the connection between personal autonomy and privacy, which enables people to act in their own best interests without interference from others. It also illustrates the connection between transparency and information availability, which is essential for effective management in the wider community, corporate, and charitable sectors. How to define the distinction between information that may be freely given to people on demand and information that needs to be limited for the purpose of safeguarding private information is the main question this book attempts to answer. The main issue is what degree of authority people ought to exercise on their private data in view of conflicting societal needs for it.

### **Objective of the Study:**

The following goals will be kept in mind as the study proceeds forward:

- The Dilemma of Privacy.
- Legislations for safeguarding data in India.
- Actions to be taken to improve data protection norms.

### **Research Methodology:**

The methodology adopted here is analytical. Both primary and secondary sources are used. The primary sources are books and e-books, secondary sources are the creative writings and

relevant materials collected from various articles, journal, newspaper and book pertinent to the study area.

### **The Dilemma of Privacy**

A person's right to privacy can be argued to be a fundamental human right that the person may assert against the government under the protection of Fundamental Rights safeguarded by Part III of the constitution. Since the inception of the age of technology, when its seeds had been sown, the problem of privacy with regard to the body parts, the internet, personality, etc., has emerged. But it was not until the 2017 judgement that this problem received media attention and the public learned about their right to privacy.

The obstacles to privacy that are discussed in Article 21 of the Indian Constitution as well as the legal understanding of an individual's freedom in light of the social system were most likely dealt with by Justice Dr. D.Y. Chandrachud in his iconic decision in *K.S. Puttuswamy v. Union Of India*, also known as the Aadhaar case. The government acquired statistics and demographic biometrics that were sensitive information for the Aadhaar programme in order to give its recipients benefit premises, which people believed may be efficiently misused with the latest technology. The Supreme Court's Bench of nine appointed judges declared the right to privacy to be an important right under part III of the constitution in this landmark decision. The application of modern technology may infringe on different individual's right to privacy.

The conflict between security and privacy has become one of the most intensely disputed worldwide concerns in the connected age of today. People are at war with one another over the opposing and divergent goals of safety and security on the one hand, and privacy and confidentiality on the other, as a result of significant data violations, fraud, malware that demands ransom, phishing scams, big brother snooping, legal abuses, and other fears.

In contemporary technologically advanced world, an individual's worries about privacy are of paramount importance. Digital technology has numerous advantages in our daily lives, yet while we appreciate these advantages, the level of information that is shared has grave privacy consequences. Although we perceive technology as being unaffected in and of itself, the effects are substantial and of tremendous magnitude. Information robotics, which has resulted in the violation of user's right, has posed a direct danger to the right to privacy in the age of technology.

The confidentiality of information in organisations is not adequately positioned to safeguard persons in relation to digital technology and privacy, even though data protection law provides the possibility to reduce the anticipatory gathering of information by organisations. Due to information technology, employers private rights are violated, and workers deal with a variety of privacy-related problems. This is due to the fact that organisations do not require evaluating staff performance at work, assessing sales, or peering over the workers. Organisations can rather maintain an eye on their workers using modern tools like laptops and emails. Emails help organisations to progress technically. The privacy of workers can become an issue when information technology is used improperly or is made available to managers. Email privacy in the United States is regulated under the Electronic Communication Privacy Act. Companies claim that they must track everything in order to improve worker performance, avoid fraudulent theft, and other dubious unlawful acts, yet this privacy infringement is criticised by workers.

In many of the instances, attaining privacy requires putting in place technologies that hinder or eliminate security. The individual must give up privacy in exchange for security and protection against dangers. By definition, maintaining privacy requires preventing tracking of a user's software, social networking sites, email, and web browsing activity. To safeguard against digital dangers, security necessitates constant surveillance and examination of such actions.

### **Legislations for safeguarding data in India**

Safeguarding of data is regarding our basic right to privacy that is protected by international and state laws and treaties. The regulation intended to safeguard our confidential data that is gathered, utilised, and kept through automated methods or is supposed to be an element of an electronic file system is known as data safeguarding. Privacy legislation is crucial in current times because they govern and direct the actions of organisations and authorities while also giving us the freedom to regulate our data while safeguarding us against misuse. Such organisations have consistently demonstrated that, without legislations limiting their behaviour, they will make every effort to gather and retain as much information as possible while keeping us in the dark.

India has a thorough and clearly established legal framework. The Information Technology Act ( IT Act) which was finally passed in 2000, comprises regulations and rules pertaining to digital crimes and security of data. The Indian Copyright Act of 1972, in addition to the IT

Act, addresses copyright issues with computer applications. Yet, many safety specialist and scholars believe that the proposed legislation fails to sufficiently safeguard personal data.

The Indian Judicial System provides certain substitute legislation along with additional protections in the lack of formal legislation. Several of the intermediary laws include:

- Sections 406 and 420 of the Indian Penal Code, which deal with the penalties for criminal trust breaches and fraudulently coercing the transfer of property, respectively.
- Breach of contract under the Indian Contract Act.

By implementing Articles 19 and 21, legal activism has included the right to privacy inside the umbrella of fundamental rights. The right to privacy has been acknowledged by the judiciary as a prerequisite for the rights to life as well as individual liberty. In *Kharak Singh v. State of Uttar Pradesh*, particularly the minority judgement of Subba Rao, J, the Supreme Court of India defined the right to life as encompassing the right to an adequate existence.

### **Actions to be taken to improve data protection norms**

Many of the top firms in the globe are now built on the data collected from our private equipments, our online transaction history, and information from different places. The commercial usage of sensitive information has expanded like the West during the last twenty years. But this expansion is gradually limiting due to users dissatisfaction, governance, and contention for users. Despite the fact that the data came from the private actions of consumers, it was treated as business asset and an official property.

Nowadays, each nation within the globe has started to view sensitive information as a possession belonging to citizens and kept in confidence by organisations, rather than as something which can be easily collected. It will serve the digital marketplace as an extremely greater structuring concept. Providing people greater authority might curb the company's darkest abuses and spark an emerging era of client-centered development as people start to indicate the kinds of customisation and possibilities they would prefer their personal information to facilitate.

Organisations have to rebuild their data processes on the altered guiding principles of approval, knowledge, and mobility in order to successfully make this change. Major organisations have started to adjust to the changing situation as it emerges. The modifications



add new data problems in addition to those currently faced by existing organisations. Numerous rivalries over client data still exist in almost all major companies. This situation will not be accepted for an extended period in the new data environment. Personal information must be obtained, talked about, safeguarded and used for financial gain properly if the company is to derive any advantage from it.

### **Conclusion:**

Technology has advanced to the point where computers are now an integral part of our daily lives and where no data provided can ever be totally confidential. From our early days to the establishment of complete companies globally, we have come a long way. Our reliance on technology has grown over time and will keep on increasing with constantly developing growth

Our private data is needed nowadays for safety reasons. We all offer the accurate data requested by the legitimate institutions. We give the data on the understanding that it is secure and will not be disclosed to any unidentified outsider without our consent.

Despite the fact that technology is advancing to new elevated positions, our nation still lacks legislation expressly addressing the harmful internet data safety. With the growing popularity of the Internet for diverse purposes and the enormous growth in technology, an entirely novel danger to the States has evolved that cannot be countered by military power. In this age of digital technology, the government can consider multiple applications that will enhance modern surveillance expertise and modernise legislative operations with the kind of greater results and thorough procedures that the present administration requires. By operating security applications on a distinct network and isolating the undesired information, the government should work with foreign technology massive corporations to manage digital information and govern it without violating the privacy of any individual. A novel legislation that focuses primarily on the safeguarding of information and data found online is the pressing requirement of the moment.

### **Bibliography:**

Floridi, Luciano. *Protection of Information and the Right to Privacy – A New Equilibrium?*. Springer International Publishing Switzerland, 2014

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York University Press, 2004



Stefanick, Lorna. *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World*. AU Press, Athabasca University, 2011

“Right to Privacy in Digital Era: A Study with Indian Context”

<https://www.legalserviceindia.com/legal/article-5404-right-to-privacy-in-digital-era-a-study-with-indian-context.html>

“The Right To Privacy In The Age Of Information Technology”

<https://www.legalserviceindia.com/legal/article-9142-the-right-to-privacy-in-the-age-of-information-technology.html>

“Right to Privacy”

<https://byjus.com/free-ias-prep/right-to-privacy/#:~:text=Right%20to%20Privacy%20E2%80%93%20Article%2021&text=According%20to%20this%20article%2C%20every,by%20the%20Indian%20Penal%20Code.>

“Right To Privacy Under Article 21 and the Related Conflicts”

<https://www.legalservicesindia.com/article/1630/Right-To-Privacy-Under-Article-21-and-the-Related-Conflicts.html>

“Technology : a threat to privacy”

<https://blog.ipleaders.in/technology-threat-privacy/>

“The Privacy vs Security Conundrum”

<https://zvelo.com/the-privacy-vs-security-conundrum/>

“Data Protection Laws in India”

<https://www.indialawoffices.com/legal-articles/data-protection-laws-in-india>

“The New Rules of Data Privacy”

<https://hbr.org/2022/02/the-new-rules-of-data-privacy>