IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022

Analyze The Implications of Technological Advancements on Privacy Rights and The Adequacy of Existing Legal Frameworks

Amandeep Kaur, Rajveer Kaur
Guru Kashi University, Talwandi Sabo

ABSTRACT

Due to the extensive gathering and use of personal data, privacy breaches are pervasive in today's data-driven world. Surveillance technology and algorithms are employed by governments, companies, and other entities for the purpose of tracking individuals, profiling marginalized groups, and censoring online content. These actions worsen discrimination and exploitation while undermining the right to privacy. Although there are legal structures in place to address these challenges, their effectiveness varies, and legislative efforts are frequently outpaced by technology improvements. Technologies that protect privacy, such anonymization and encryption, are viable ways to reduce privacy threats and allow for the proper use of data. To guarantee a balanced strategy that puts privacy, security, and individual liberty first, their adoption calls for cooperation and supervision. Thus, resolving the intricate relationship between technology and privacy rights requires a variety of approaches, including legislative changes, technological advancements, and raising public awareness.

Keywords: *Technological, Advancement, Privacy Rights, Privacy Laws, Framework.*

1. INTRODUCTION

We are profiled as members of contemporary society. We understand that we must provide personal information to the appropriate authorities, and we trust that they will protect this data, using it only in the most extreme and legally justified instances. Governments receive information about children from their parents in order to provide essential services, such healthcare. Every time we sign a form or click a button, we are effectively giving up some personal information. This increases the risk of our data being used for illegal purposes because it allows for the resale of our personal information.

Many of the time, detecting devices follow our every move, save our preferences, and collect any data they can find about us online—all without our knowledge or permission. People use this data to legally discriminate against us, steal from us, and manipulate us. All of us are being followed by algorithms that create profiles. This isn't some paranoid, gloomy vision of the future. Here we are in the present, in a data-driven culture where corruption is pervasive and a select few are able to exploit the plight of the masses who rely on the internet and mobile phones for their news and entertainment **[1]**.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022

2. PRIVACY VIOLATIONS

a. Search and Seizure of Digital Property

Regarding privacy rights and legal protections, the subject of digital property search and seizure in India presents serious concerns. While there are laws protecting physical property, such homes and possessions, from unlawful access, the legal structure for digital property is still largely insufficient and less clear. There have been reports of instances where police enforcement and government agencies have accessed people's digital devices and online accounts without the necessary authorization or supervision, which may have resulted in privacy rights violations. These problems are further made worse by the absence of precise rules and regulations controlling digital search and seizure practices, which leaves people open to arbitrary intrusions into their digital life. To tackle this issue, extensive legislative framework reforms in India are necessary **[2]**. These reforms must guarantee that people's digital privacy rights are sufficiently protected, and that there are explicit protocols and security measures in place for actions involving searches and seizures.

b. Profiling of Marginalized Groups

Profiling people who belong to marginalized groups increases social inequality and is a serious danger to privacy. Law enforcement agencies have been known to engage in discriminatory profiling of marginalized communities on the basis of socioeconomic status, religion, and ethnicity. This practice has resulted in disproportionate targeting and harassment of these communities. These worries are heightened by the use of technology, particularly data mining and surveillance, which makes it possible to track and profile members of marginalized groups in a systematic manner. Furthermore, these problems are made worse by the absence of strict laws and oversight procedures, which permits the biased and capricious application of profiling methods. In order to meet this problem, India's legal system needs to be completely reformed to guarantee that profiling operations are carried out openly and in compliance with the non-discrimination and equality standards **[3]**. Furthermore, in order to create a society that is more inclusive and equitable, it is imperative that initiatives to raise public and law enforcement understanding and sensitivity regarding the effects of profiling on marginalized communities be made.

c. Biometric Dangers

There are serious privacy and security issues with the widespread use of biometric technologies, especially when it comes to the gathering and storing of sensitive personal data. The use of biometric data, such as fingerprints and iris scans, for identification and verification is increasing due to the introduction of programs like Aadhaar, which require biometric authentication for a number of services and benefits. The centralized gathering and archiving of biometric data, however, raises questions around data breaches, misuse, and illegal access, putting people's security and privacy at serious danger **[4]**. Furthermore, these risks are made worse by the absence of strong legislative protections and supervision procedures, which exposes people to

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022

possible misuse and exploitation of their biometric data. In order to address these biometric risks, India's legal system must be completely reformed. Strict guidelines and protections for the gathering, storing, and use of biometric data must be provided, as well as channels for responsibility and redress in the event of misuse or breaches. Protecting privacy rights in India also requires initiatives to increase public knowledge of the dangers of biometric technology and to encourage greater accountability and transparency in their use.

d. Censorship

Freedom of expression and information access are seriously hampered by censorship, especially in the digital sphere. Although the nation has a thriving media environment and strong legal protections for freedom of speech and expression, there have been cases of censorship by the state and private organizations to limit access to online information that is considered offensive or provocative. There are worries that censorship may go too far and that dissenting opinions may be silenced when laws like the Information Technology Act and sections of the Indian Penal Code are used to restrict expression online. The threat to freedom of expression and access to information in India is further highlighted by the rise of social media bans and internet shutdowns in response to communal disturbances or civil upheaval. In order to combat censorship, it is important to strike a careful balance between defending fundamental rights and maintaining national security **[5]**. Additionally, there should be more responsibility, openness, and adherence to the law when it comes to regulating online content. In order to enable citizens to critically assess online content and stand up for their rights to free speech and expression in the digital age, it is imperative that initiatives to advance media and digital literacy be made.

e. Business Surveillance

Business monitoring raises serious issues with data protection and privacy rights, especially in light of how frequently businesses gather and use personal information. Businesses now have access to enormous volumes of customer data, including behavioral patterns and personal information, thanks to the quick digitization of many industries and the growing reliance on digital platforms for communication and commerce. However, questions are raised about the possibility of abuse or illegal access, as well as the openness and consent procedures controlling the gathering and use of this data. Strong legislative frameworks and monitoring procedures are required to control corporate surveillance tactics and safeguard people's right to privacy in light of incidents of data breaches and privacy violations by corporations. Transparency, accountability, and trust in the digital economy also depend heavily on initiatives to raise consumer knowledge and provide people more control over their personal data **[6]**.

3. TECHNOLOGICAL ADVANCEMENTS AND PRIVACY RIGHTS

The creation of digital tools for control and surveillance is often believed to be the most significant issue with privacy in today's postmodern culture **[7]**. The issue of how to legally safeguard personal information against technological intrusions remains unresolved. Actually,

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022

"the landscape on which laws are made" has been considerably altered by technological advancements. The ongoing evolution of technology has made the already formidable challenge of incorporating it into existing legal frameworks, which dates back to the 1970s, all the more daunting. Constantly evolving technology brings with it new opportunities for "miniaturisation, convergence, interoperability and ubiquity," all of which must be addressed.

To provide just one example, the right to private correspondence guaranteed by the European Convention on Human Rights is particularly vulnerable in the modern day. Letters were the primary means of communication before the development of the telephone. These days, it might also mean email and SMS messaging. Nowadays, it's really difficult to maintain privacy due to electronic media. It will be extremely difficult to legislate away the new surveillance technologies and databases, regardless of the number of laws that are enacted. This is the fundamental issue with the ongoing conflict between technology and privacy legislation. Their presence is permanent. Because of this, we need to shift our viewpoint and look at the issue from a different angle if we want to solve it **[8]**. The technology is not inherently problematic; rather, it may be our misuse of it. We must confront "uncomfortable and far-reaching choices among conflicting interests and basic social values" if we are to find solutions to our current issues, and James Rule argues that blaming technology is the incorrect strategy.

To begin, regulating transparency is essential in protecting the right to privacy in the modern day. The establishment of a just and democratic system of control necessitates, among other things, a system that is fairly visible, so that citizens are not surreptitiously watched and everyone can see and control who sees their data. Careful legal regulation, bearing in mind human rights concerns, should govern control. Without taking into account all relevant circumstances, it will be impossible to strike a fair balance between privacy and security concerns. A democratic and compassionate application of control technology is required. So, there's no problem with utilizing technology to keep people safe, but we need to make sure it doesn't impede their freedom too much. Unfortunately, technology is frequently utilized for immoral reasons, which not only infringe upon privacy but also deprive persons of their agency **[9]**. The manner in which people are watching us are frequently invisible to us. Our fear stems from our complete lack of knowledge. Thus, regulations on the use of technology for control should be designed to make it easier for us to have more control over our lives, rather than putting our actions at risk.

4. PRIVACY-PRESERVING TECHNOLOGIES: AN OVERVIEW

Protecting private data while allowing its efficient use is the goal of privacy-preserving technologies, which cover a wide range of approaches. Johnson et al. states that these technologies have a multi-faceted scope and are essential for reducing privacy issues in digital contexts. One of the cornerstones of privacy protection is encryption, which makes data unintelligible without the key to decipher it. Even in the case of illegal access, our methodology guarantees confidentiality **[10]**.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022

In order to protect individuals' identities while still enabling their legitimate analysis and use,anonymization is defined by Patel and Jones as the process of removing or altering recognizable components inside databases. By adding noise or randomness to query responses, differential privacy—first proposed by maintains statistical correctness while protecting the privacy of individual contributions inside datasets. This section presents privacy-preserving approaches in a structured manner, outlining their many types and demonstrating how well they work. Secure data transmission and storage is achieved through the use of encryption approaches, which include symmetric and asymmetric encryption schemes. For data publication and sharing, anonymization methods like k-anonymity and l-diversity come into play.

The efficacy and practical application of these technologies in various contexts are demonstrated through case studies. One example is the use of homomorphic encryption in healthcare data sharing, which has proven to be effective in protecting confidentiality while yet allowing for full analytical capabilities **[11]**. Furthermore, the use of differential privacy in large-scale data aggregation demonstrates its potential to safeguard individual privacy while facilitating valuable data analysis.

5. EXISTING LEGAL FRAMEWORKS FOR PRIVACY PROTECTION

Unlike the United States and the European Union, India does not have a data protection law. As a result of a dearth of data protection legislation, privacy and property rights are used to achieve data protection in India. Both the Indian Constitution and the Information Technology Act of 2000 guarantee citizens' right to privacy. The Indian Penal Code of 1860, the Copyright Act of 1957 **[12]**, and the Indian Contract Act of 1872 all address property rights. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were enacted by the Indian Ministry of Communication and IT (Lok Sabha Secretariat, 2013) **[13]**. In order to comply with these regulations, businesses must collect, process, and store customers' personal information. Specific personal information, including sensitive data, is collected in order to carry out the specified procedures.

5.1. Status of Data Protection and Privacy Rights in India

One of the basic rights guaranteed by the Indian Constitution is the right to personal privacy, as stated in Article 21 **[14]** and other relevant clauses. No individual in India may be deprived of life or liberty without due process of law, according to Article 21 of the country's constitution. The right to privacy is a part of the right to life and the right to personal liberty, as the Supreme Court has made clear in multiple instances.

But you can't sue private individuals or groups for violating your constitutional rights. The only entities that can be sued for these are the state or entities owned by the state. Sections 43(a)–(h) and 65–74 of the Information Technology Act, 2000 address cyber violations and offenses, respectively. In order to commit cybercrimes, one must obtain unauthorized access to computer systems or networks in order to steal data. In India, such violations might result in civil prosecution. Hacking with the purpose to destroy the system, meddling with computer source

code, and breaching privacy and secrecy are all examples of cyber crimes. Prosecution for these cyber offenses is facilitated by the IT Act. Such violations are likewise punishable by law according to the Information Technology Act of 2000.

Any breach of confidentiality involving third-party data may result in legal action against the relevant network service provider or intermediary under the IT Act. Inadequate vigilance in preventing the crime is also its responsibility. According to the IT Act, an intermediary is a third party that receives, stores, transmits, or offers service in relation to an electronic message on behalf of another party. Therefore, as a service provider, an outsourcing firm can face legal consequences **[15]**. The IT Act's reach extends across national borders as well. Offenses and violations committed outside of India are encompassed. Crimes committed by Indians or foreigners are equally serious. That the relevant computer system or network be situated in India is the sole stipulation.

6. CONCLUSION

The contemporary digital environment poses previously unheard-of obstacles to individuals' right to privacy, calling for a review of current legislative frameworks and the use of technology that protect privacy. Many times, without the subject's knowledge or agreement, the widespread gathering and use of personal data gives rise to serious worries about discrimination, profiling, and monitoring. Governments and businesses have a great deal of ability to monitor and manage people's digital lives, which can result in censorship, surveillance, and exploitation that mostly affects marginalized populations. There are legal protections, such as data protection legislation and constitutional rights, but different jurisdictions have different standards for their sufficiency and enforcement. Furthermore, the necessity for proactive steps to protect privacy rights in the digital era is highlighted by the fact that legislative attempts are consistently outpaced by the rapid advancement of technology. Technologies that protect privacy, such as differential privacy, anonymization, and encryption, are viable ways to reduce privacy concerns and allow for the proper use of data. To guarantee a balanced strategy that prioritizes privacy, security, and individual autonomy, legislators, technologists, and civil society must work together to facilitate their widespread adoption. Thus, in order to protect basic rights in the face of changing digital problems, tackling the complex interplay between technological improvements and private rights requires a holistic strategy involving legal changes, technological innovations, and societal awareness.

REFERENCES

1. Flock, Elizabeth. "What Internet censorship looks like around the world". Washington Post. April 5, 2012: https://www.washingtonpost.com/blogs/blogpost/post/internet-censorship-whatdoes-it-look-like-around-theworld/2012/01/18/gIQAdvMq8P_blog.html?utm_term=.d0ebce509827.
2. Asher, Jeff and Arthur, Rob. “Inside the Algorithm That Tries to Predict Gun Violence in Chicago”. The New York Times. June 13, 2017:

https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagoshigh-risk-list.html.

3. Patton, D. U., Brunton, D. W., Dixon, A., Miller, R. J., Leonard, P., and Hackman, R. (2017). Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. Social Media+ Society, 3(3), 2056305117733344: http://journals.sagepub.com/doi/full/10.1177/2056305117733344.
4. Human Rights Watch. "China: Police 'Big Data' Systems Violate Privacy, Target Dissent" November 19, 2017: https://www.hrw.org/news/2017/11/19/china-police-big-data-systemsviolate-privacy-target-dissent.
5. Tribunal Superior Eleitoral. "Biometria". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/biometria.
6. Tribunal Superior Eleitoral. "Parceria entre TSE e PF visa maior eficiência da gestão pública". Setor de Administração Federal Sul (SAFS): http://www.tse.jus.br/imprensa/noticiastse/2017/Novembro/parceria-entre-tse-e-pf-visa-maior-eficiencia-da-gestao-publica.
7. A. T. Keynon, and M. Richardson eds., New Dimensions in Privacy Law, Cambridge University Press, Cambridge 2006, 11. Council of Europe, New Technologies: a challenge to privacy protection?, Legal Affairs, Strasbourg 1989, 5.
8. S. Gutwirth, et al., Computers, Privacy and Data Protection: an Element of Choice, Springer, Brussels 2011, v 9 European Convention on Human Rights, http://www.echr.coe.int/documents/ convention_eng.pdf, last visited 01 December 2014.
9. D. Brin, The Transparent Society: Will Technology Force Us to Choose Between Privacy and Feedom,? Addison-Wesley, Reading 1998.
10. Gupta, S., & Wang, J. (2021). k-Anonymity and l-Diversity in Data Sharing Scenarios. International Journal of Data Privacy, 9(4), 320-335.
11. Johnson, R., et al. (2018). Privacy Risks Mitigation in Digital Environments. Journal of Privacy Technology, 14(2), 180-195.
12. Indian Copyright Act (1957). URL: http://copyright.gov.in/documents/copyrightrules1957.pdf.
13. Lok Sabha Secretariat (2013). Committee on Subordinate Legislation, 31st Report. Presented on 21.03.2013. Fifteenth Lok Sabha, New Delhi. URL: http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
14. Jani, N. (2013). Article 21 of the Constitution of India and Right to Livelihood. Voice of Research, Volume 2, Issue 2, September 2013, ISSN No. 2277-7733.
15. Law Commission of India (1997). One Hundred Fifty-Sixth Report on The Indian Penal Code, Volume II, August 1997. URL: http://lawcommissionofindia.nic.in/101-169/Report156Vol2.pdf.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 11, S.Iss 06, 2022