RIGHT TO PRIVACY IN THE DIGITAL AGE

Mudita Sharma, Gautam Buddha University

ABSTRACT

The Right to Privacy has been developing as an inseparable part of human dignity and autonomy, which has acquired a new meaning in the age of the digital realm. As the number of data-driven technologies increases exponentially, privacy is a precarious and disputed right and every day individuals create, transfer, and store personal information on the internet. Pervasive surveillance, data mining and algorithmic profiling are some of the defining features of digital era, and have eliminated the distinction between the personal and the political life.[1] The use of advanced systems to gather individual data in the pretext of security and convenience is growing by governments and corporations at the cost of informational self-determination of citizens. The landmark lawyer John Justice K.S. Puttaswamy (Retd.). v. Privacy was identified as a fundamental right by the union of India under art. 21 in the Indian constitution reinforcing its constitutionality in the wake of technological difficulties.[2] Nonetheless, this is not true because the lack of holistic data protection laws and the emergence of digital authoritarianism still pose threats to the privacy rights of people around the world. The appropriate balance between innovation, national security and individual freedoms is the only way of providing proper protection of privacy. Privacy identification and implementation in the virtual environment are not just a legal requirement but a moral obligation that is necessary in protecting the democracy and human rights in the era of information.[3]

Keywords: Privacy Rights, Data Protection, Digital Surveillance, Fundamental Rights, Information Technology Law.

[1] Daniel J. Solove, *Understanding Privacy* 8–10 (Harvard Univ. Press 2008).
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[3] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).

INTRODUCTION

The sudden development of the digital technologies has transformed the manner in which people engage, communicate, as well as the manner in which people carry on with their day-to-day tasks. The use of social media, e-commerce, cloud computing, and artificial intelligence is making massive amounts of personal data on a second-by-second basis. These technological advances have certainly brought about more convenience and connectivity of the world but, at the same time, they have become a serious menace to individual privacy. The Right to Privacy, which was initially perceived as a part of the individual liberty, has become one of the most significant issues concerning human rights in the twenty-first century.[4]

Governments and other non-governmental organizations continuously gather personal information, analyze it and sell it in the digital ecosystem. It is a mass surveillance that will put at risk the conventional concept of consent, autonomy, and the right to decide on what information is gathered about them. These issues have been exacerbated by the emergence of so-called big data and predictive analytics since people tend not to know what happens with their data and how the latter is being abused. The lack of transparency and accountability in the data processing further makes the implementation of privacy norms rather complicated. The historic ruling of Justice K.S. Puttaswamy (Retd.) in India. v. Union of India (2017)[5] , the privacy law, which was established by the in Article 21 of the Constitution[6], was declared by the court as a fundamental right and thus it was a constitutional right. The case brought a shift of paradigm concerning the privacy in India in line with the international human rights declarations of Articles 12 of the Universal Declaration of Human Rights[7], and 17 of the International Covenant of Civil and Political Rights[8].

Nevertheless, the legal and policy frameworks are still underdeveloped in response to the modern digital threats, despite the legal recognition. Unregulated gathering of biometric information, anti-international cyber spy, and overseas information transfers are still subjecting people to exploitation.[9]

[4] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).
[5] Supra 2.
[6] Constitution of India, art 21.
[7] Universal Declaration of Human Rights, (1948), A.12.
[8] International Covenant on Civil and Political Rights, (1966), A.17.
[9] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).

RESEARCH OBJECTIVES

The main goal of this study is to critically observe the morphing outlines of the Right to Privacy in the digital age, especially on the areas of protecting data, technological surveillance and informational autonomy. This study will aim at:

1. Examine the constitutional and the international law grounds of the Right to Privacy regarding the digital realm.

2. Evaluate the risks of the emerging technologies like artificial intelligence, social media, and analytics of big data on the protection of privacy.

3. Review the sufficiency and breadth of the existing Indian laws and compare with the information protection regulations worldwide such as the EU General Data Protection Regulation (GDPR).

RESEARCH QUESTIONS

1. What has changed is the Right to Privacy and its Constitution in India and how do the changes keep with the international standards of human rights in the digital world?

2. What do we define as the most significant threats to individual privacy experienced due to technological development like artificial intelligence, social media surveillance and data analytics?

3. How much do current laws and policies on data protection in India stop the informational privacy and what changes are necessary in order to make them stronger and more futuristic?

HYPOTHESIS

The research hypothesis is that although the Constitutionally guaranteed Right to Privacy has already been established as the fundamental right in India, the current legal and policy frameworks cannot be considered sufficient in modern times to protect the right due to the digital era. The hearing must be re-evaluated even though the judiciary has affirmed the same in Justice K.S. Puttaswamy (Retd.). v. Union of India the fact that privacy is inherent to life and liberty in Article 21 of the Constitution, effective implementation is still challenged by

poor legislation and the dynamic wave in technology. This assumption is that the informational autonomy has been jeopardized due to unchecked data gathering, surveillance technology and algorithmic profiling and thus the existence of individual freedom and dignity is subverted.[10] Further, there is no threshold data protection regulations that match the EU's General Data Protection Regulation (GDPR), and this is another factor that creates privacy exposures in the digital world of India.[11] Therefore, the research paper hypothesizes that an effective legal system is necessary to facilitate the implementation of the privacy rights in the digital era.

RESEARCH METHODOLOGY

The approach of this research study is a qualitative and doctrinal methodology, which concentrates on the critical analysis of all the legal principles, judicial decisions, and statutory provisions that construe the Right to Privacy in the digital age. It is more of a doctrinal study since it is based on the interpretation of the current legislation, the clauses in the constitution, as well as authoritative judicial ruling that formulated the legal concept of privacy in India and across the world.[12] Another methodology used in the research is comparative as the privacy framework in India will be contrasted with the international regulatory standards, including the European Union General Data Protection Regulation (GDPR) and the domestic data protection regulations on sectors in the United States, and gaps in legislative and structural provisions to identify the gaps in privacy regulation in India.

In the study, both primary and secondary sources have been used. Primary sources are provisions of the constitution, laws (statutes), case law and even some international legal documents like the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966). The secondary sources will include books, scholarly journals, research articles, state reports, and reputable internet databases as a way of obtaining in-depth information on developing privacy strata of jurisprudence.[13]

[10] Daniel J. Solove, *Understanding Privacy* 25–28 (Harvard Univ. Press 2008).
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[12] C.K. Takwani, *Lectures on Administrative Law* 33–34 (Eastern Book Co. 2020).
[13] K.N. Chandrasekharan Pillai, *Constitutional Law of India: Principles and Practice* 412–415 (Eastern Book Co. 2021).

LITERATURE REVIEW

The Right to Privacy has been widely discussed both in scholarly and judicial literature, developing into a concept of a very limited scope regarding physical isolation to a large scope of informational and digital freedom. Privacy has a long history of being theorized in academia, with the first such seminal contribution being the seminal article, The Right to Privacy (1890) by Warren and Brandeis, which formulated the conceptualization of privacy as the freedom to be left alone and was concerned with the threat of invasive media and technology.[14] Their formulation gave intellectual foundations to later judicial and legislative developments to the privacy jurisprudence.

This was further enhanced by Alan Westin in his book, Privacy and Freedom (1967) which pointed out privacy as the right of an individual to control any personal information and that they should determine when, how and to what extent information about them should be shared with others.[15] The theory became especially applicable in the digital era when the constant sharing of personal information undermines limits of consent and informational control.

Privacy had not been well-developed as a discourse in the Indian context until the seminal ruling of the Supreme Court wrote in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[16], it was unanimously accepted by the established principle of privacy as a fundamental right under Article 21 of the Constitution. The decision relied on relative constitutional principles and the international human rights law and affirmed that privacy is inseparable with human dignity and individual freedom.

Legal theorists like Daniel J. Solove claim that threats to privacy today are no longer rooted in single encroachment, but rather a systemic data processing and surveillance mode of practice that generates long-term damaging informational effects.[17]

In addition, the Report of the United Nations Human Rights Council on The Right to Privacy in the Digital Age (2014) demonstrated the increasing worldwide interest in governmental

[14] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).
[15] Alan F. Westin, *Privacy and Freedom* 7–8 (Atheneum 1967).
[16] Supra 2.
[17] Supra 1.

surveillance and exploited corporate data.[18]

ANALYSIS

CONSTITUTIONAL AND INTERNATIONAL FRAMEWORK OF PRIVACY IN THE DIGITAL AGE

The notion of the Right to Privacy has been embraced to become one of the foundations of constitutional and human rights jurisprudence in the global area. Conventionally based on the concept of personal autonomy and dignity, privacy has been rediscovered in the digital world, where people are increasingly being subjected to surveillance, data profiling, and data processing without first seeking their consent.[19]

Constitutional Framework in India.

The constitutional basis in ensuring privacy protection in India is majorly on Article 21 of the Constitution that details the right to life and personal liberty. First, the Indian courts failed to appreciate privacy as a constitutional right. In M.P. Sharma v. Kharak Singh (1962) and Satish Chandra v. State of Uttar Pradesh (1954),[20] the Supreme Court declared that the Constitution did not mention that privacy was secure.

The result of this development was the seminal case of nine judges on the bench in Justice K.S. Puttaswamy[21], figure that unanimously stated that the Right to Privacy is a constitutionally secure right inherent to life and liberty. The Court has found privacy to be comprised of physical, informational, and decisional autonomy and a paramount quality of human dignity.

The Puttaswamy court ruling also highlighted the policy requirement of protecting the misuse of personal information and unreasonable surveillance by enacting legislative protection. The logic of the Court provided a foundation towards the further attempts to introduce a complete data protection law in India. One of the major progress points is the introduction of the Digital Personal Data Protection Act, 2023[22], which leads to the harmonization of the domestic privacy

[18] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[19] Supra 10.
[20] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[21] Supra 2
[22] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

system in India with world standards, but the scale of its provisions and application is still questioned.

International Legal Framework

Privacy has been identified as a universal human right at the international level. Article 12 of the Universal Declaration of Human Rights (UDHR) (1948) and Article 17, of the International Covenant on Civil and Political Rights (ICCPR) (1966) both confirm the right of the individual to protection against arbitrary interference establishing privacy, family, home or correspondence.[23]

The General Data Protection Regulation (GDPR) is the most detailed legal document concerning personal data security in the digital scenario in the European Union. It offers people enforceable rights like data access, data rectification and portability as well as the right to forget and puts responsibility and liability on the data controllers and processors, making data management more accountable and transparent.[24]

In its reports on The Right to Privacy in the Digital Age (2014, 2021), the UN Human Rights Council has stressed that the mass gathering of data without adequate performance of protection of data would be against the tenets of lawfulness, necessity, and proportionality.[25] In the same way, the Convention 108 (1981), the first binding international convention on data protection, which was issued by the Council of Europe, created a framework towards cross border data privacy, India being a signatory to the UDHR and ICCPR[26] has a duty to assure adherence of the international standards to the domestic laws.[27]

THREATS TO THE RIGHT TO PRIVACY IN THE DIGITAL AGE

The physical world has also changed interaction, commerce, self-governance and reorganization among people by providing unprecedented access to information and technology through the digital age. However, the lines between the personal and the

[23] Universal Declaration of Human Rights, art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948); International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
[24] Supra 1.
[25] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[26] International Covenant on Civil and Political Rights, art. 2(1), Dec. 16, 1966, 999 U.N.T.S. 171.
[27] K.N. Chandrasekharan Pillai, *Constitutional Law of India: Principles and Practice* 423–425 (Eastern Book Co. 2021).

professional have vanished in the face of the spread of social media, big data analytics, artificial intelligence (AI) and surveillance technologies which make people more vulnerable to on-line intrusions.

State Intrusion and Data Surveillance

Government surveillance of masses is still one of the most serious threats to privacy. Although surveillance is usually done on the premise of national security, law and order, and prevention of crime, random gathering and interception of communication should arouse serious considerations about the constitution.

In India, surveillance by the state is legally empowered by a number of laws, including, prominent among them, Section 5(2) of the Indian Telegraph Act, 1885, which allows interception of communications in the interest of their own safety, and Section 69 of the Information Technology Act, 2000, which gives the government the authority to monitor, decrypt, and intercept any digital communications and data in the name of its national security or protecting its citizens.[28] Some of the state surveillance programs that enable it to do so include the Central Monitoring System (CMS), Network. According to critics, there is no sufficient judicial check and legislative protection on how these systems work.[29]

The necessity to impose severe restrictions on state surveillance is additionally supported by world events. Likewise, the revelations of Edward Snowden (2013)[30] exposed the extensive surveillance initiatives by the U.S. National Security Agency (NSA), which have caused concern in other parts of the world, including India, where the Aadhaar biometric system and other databases of e-governance are being feared as profilers and abusers of personal data.

Digital Exploitation and Corporate Data Mining.

Corporate areas are also involved in extensive data mining and profiling other than by the State. Leveraging social media, e-commerce, and mobile apps, technology firms are collecting

[28] Indian Telegraph Act, No. 13 of 1885, § 5(2) (India); Information Technology Act, No. 21 of 2000, s. 69 (India).
[29] Internet Freedom Foundation, *The State of Surveillance in India* (2023), available at https://internetfreedom.in.
[30] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books 2014).

personal data to create a behavior profile and targeted advertisements. This kind of data collection may be done without express permission or accountability.

The case of Cambridge Analytica scandal (2018)[31], in which millions of Facebook users were profiled to sell political ads, served as an excellent example of how humanity data can be used commercially by companies without following the proper democratic procedures, a scenario that therefore was somewhat described by scholar Shoshana Zuboff as surveillance capitalism where human experience becomes raw material to be used commercially.[32]

LEGAL SAFEGUARDS AND JUDICIAL APPROACH TO PRIVACY PROTECTION IN INDIA

The jurisprudential title of privacy in India started with the law case of M.P. Sharma v. In Satish Chandra[33], the Supreme Court declared that unauthorized surveillance and domiciliary visits to the police did not infringe the right to privacy provided in the Constitution, which had no such right, so it stated in its ruling, *Kharak Singh v. State of Uttar Pradesh*[34].It was the first court to identify privacy as an important part of personal liberty under the Constitution.[35]

In Justice K.S. Puttaswamy (Retd.). v. Union of India, the Supreme Court in a 9-judge Court decided unanimously that the right to privacy was an inherent right to life and personal liberty within Article 21of the constitution.[36] This overturned the ruling in M.P. Sharma and Kharak Singh on the ground that they held that there was no constitutional right to privacy.

In addition to the constitutional protection, there are various statutory protections in the form of the laws. Section 43A[37] of the Information Technology Act, 2000 (IT Act) is a compensation body to the failure to protect data by corporate bodies which deal with sensitive personal information. Section 72[38] of the Act is another penal provision whereby failure to provide protection on data obtained during line of duty is compensated.

[31] *Cambridge Analytica Data Scandal: Facebook's Role in Political Profiling*, BBC News (Mar. 2018).
[32] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).
[33] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[34] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[35] Id. at 1303 (Subba Rao, J., dissenting).
[36] Supra 2.
[37] Information Technology Act, 2000, S. 43A (India).
[38] Id. S. 72.

CONCLUSION

The acknowledgment of the right to privacy as one of the fundamental rights in Justice K.S. Puttaswamy (Retd.) v. Union of India[39] was a constitutional milestone in the Indian jurisprudence. The case has changed privacy into a peripheral concept to that of human dignity, liberty and autonomy. With the era of digital technologies and the generation of personal data constantly, its collection, and monetization, privacy has already become a civil right as well as an economic requirement. The trick is, however, that it is difficult to operationalize this right in the fast developing technological context, where mass surveillance, algorithmic profiling, and opaque data ecosystem become the established norm.

India has had a mixed electro magnificence in its quest to achieve all-encompassing privacy protection in the form of judicial activism and judicial reform. Although the adoption of the Digital Personal Data Protection Act, 2023 is a right step, it is necessary to ensure its effectiveness through enforcement, institutional independence, and actual accountability systems as well as longer-term reliance on the principles of the fundamental right of privacy.

Judicially, the institution of informational privacy of the Supreme Court along with its proportionality, lawfulness, and necessity requirements offer a solid tool of regulation of individual rights and the establishment of legitimate State interests to prevent the inevitable undermining of the privacy through legal authorities which may be abused by the powerful executive.

To sum up, privacy as a right in the digital world is not only legally justified but social. The decision to uphold it requires the concerted efforts of the judiciary, legislature, civil society, and individuals. Protection of privacy should also be dynamic as technology keeps changing, because it will keep human dignity and autonomy at the forefront, rather than the need to spying and selling data.

[39] Supra 2.

BIBLIOGRAPHY

Cases

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
2. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).
3. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).
4. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).
5. *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).
6. *Internet and Mobile Ass'n of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India).

Statutes and Legislations

1. The Constitution of India, 1950.
2. Information Technology Act, No. 21 of 2000, India Code (2000).
3. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
4. Indian Telegraph Act, No. 13 of 1885, India Code (1885).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council, General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1.

Books

1. M.P. Jain, *Indian Constitutional Law* (8th ed. LexisNexis 2018).
2. H.M. Seervai, *Constitutional Law of India* (4th ed. Universal Law Publishing 2012).
3. Justice K. Chandru, *Right to Privacy and Data Protection in India* (Orient BlackSwan 2021).
4. Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution*

(Oxford Univ. Press 2016).

5. S. Ramaiah, *Cyber Law: Privacy and Data Protection* (Eastern Book Co. 2020).

Journal Articles

1. Usha Ramanathan, *A Right to Privacy in India*, 3 Int'l J. L. & Pol'y 35 (2019).

2. Justice B.N. Srikrishna, *Data Protection in India: The Road Ahead*, 61(2) J. Indian L. Inst. 179 (2019).

3. Apar Gupta, *Balancing Privacy and National Security in India's Digital Future*, 12 NALSAR L. Rev. 95 (2020).

4. Rina Agarwala, *Privacy, Surveillance, and the Indian State: Post-Puttaswamy Reflections*, 5 Indian J. Const. L. Stud. 67 (2021).

5. Saptarshi Mandal, *Constitutionalizing Privacy: The Indian Experience*, 14 NUJS L. Rev. 44 (2022).

Reports and Government Publications

1. Justice B.N. Srikrishna Committee Report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Government of India, 2018).

2. Ministry of Electronics and Information Technology (MeitY), *White Paper on Data Protection Framework for India* (2017).

3. National Cyber Security Policy, Ministry of Electronics & Information Technology, Government of India (2013).

4. Ministry of Electronics & Information Technology, Government of India, *Data Protection Awareness Programme* (2024).

Web Sources

1. Press Information Bureau, Government of India, "Digital Personal Data Protection Bill, 2023: Key Highlights" (2023), available at https://pib.gov.in.

2. Internet Freedom Foundation, "Privacy and Data Protection: The Indian Perspective" (2023), available at https://internetfreedom.in.

3. World Economic Forum, "The Global Risks Report 2024: Data Privacy in the Digital Era," available at https://www.weforum.org.

4. United Nations Human Rights Council, "The Right to Privacy in the Digital Age," U.N. Doc. A/HRC/39/29 (2018).

5. Organization for Economic Co-operation and Development (OECD), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (2013), available at https://www.oecd.org.