



RIGHT TO PRIVACY IN THE DIGITAL AGE: DATA BREACH, LAWS, AND LEGAL CHALLENGES IN INDIA

Dr. Garima Goutam

Assistant professor, department of law

Government Law college kota

ABSTRACT

Given India's increasing dependence on digital technology and the proliferation of online venues, a new idea of privacy has arisen in the nation. This is a consequence of the country's rising reliance on digital technology. Even if the relevance of data has increased in the digital age, there are still significant worries over people's privacy due to the ubiquity of data breaches and the exploitation of data. The right to privacy, which was recognized as a fundamental right under Article 21 by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017), has taken on a greater relevance as a result of the development of cybercrimes, identity theft, and illegal surveillance. A number of new laws, including the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023, have been enacted in India as a reaction to the risks that have been identified. On the other hand, there are still gaps in public comprehension, accountability on the part of digital service providers, enforcement, and protection of data across international borders. The present privacy legislation, the challenges of striking a balance between technological innovation and data security, and the pressing need for a robust data protection framework to ensure that people have faith in the internet are all topics that are discussed in this paper.

Keywords: Right to Privacy, Data Breach, Digital Age, Data Protection Laws, Legal Challenges, India.

INTRODUCTION

It is the technical infrastructure of a civilization that serves as the motor that drives every civilization toward advancement. As a result of its engagement in a diverse variety of sectors, such as healthcare, banking, and communication, it has been of assistance to mankind in bringing about social change and progress. There has been a significant surge in the digital revolution in the 21st century, and India is not an exception to this trend. Similar to other countries, India has the biggest concentration of people who use the internet. "Digital India" is a program that was recently announced by the government of India, which took this into account. As a result of the "Digital India" movement, our rights, especially our right to privacy, are being challenged. This is despite the fact that there are multiple advantages to processing personal data via the use of various electronic devices and applications. On a daily basis, individuals, organizations, and government agencies collect personal information via a number of methods. These methods include the internet as well as the many programs and forms that users utilize on their various electronic devices. When individuals utilize their electronic devices for activities such as playing games

online, filling out applications for government or private services, posting on social media, making purchases online, submitting resumes to employment sites, buying sim cards or phone connections, and other similar activities. We are required to supply essential personal information in order to take part in any of these activities. This includes our full name, address, phone number, email address, entire address, location, friends list, and other relevant information. Because of the ease with which advertisers and organized criminals may get access to the data and information that consumers have freely contributed, these persons may misuse the access they have been granted. This not only breaches people's right to privacy via various technical ways, but it also demands for the establishment of data protection regulations.

Right to Privacy and Data Protection

The "Right to Privacy" of an individual enables them to reside in relative safety by themselves. In the majority of instances, it gives individuals the option to decide whether or not to disclose personal information. In its most fundamental form, it refers to the liberty to interact with certain persons. As a matter of fact, it enables us to determine which components are available to other individuals and to control the extent, manner, and timing of the use of those components that we disclose. It is against the law for anybody to disclose information on an individual to the general public without first obtaining permission from the individual for doing so. In the event that someone was to behave in this manner, they would be violating the rights of another individual and might be subject to legal action for damages. The right to privacy has been recognized as a fundamental right by a number of international instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights, the United Nations Convention on the Protection of Children, and the International Convention on the Protection of All Migrant Workers and Members of Their Families. These are just some of the fundamental rights that have been recognized.

In contrast to the International Instruments, the Indian government does not acknowledge the existence of a separate right to privacy or confidentiality. This right was created by a series of decisions on the part of the Supreme Court, starting with the well-known "Auto Shankar's Case" (R. Rajagopal v. State of Tamil Nadu), and it is actually included into Article 21 of the Constitution of India. In this section of his memoirs, Auto Shankar, who was incarcerated at the time for a number of murders, discussed his interactions with a large number of Indian Administrative Service (IAS), Indian Police Service (IPS), and other law enforcement agents. Several of them were among his accomplices in illegal activity. In this instance, the editor of the Tamil magazine "Nakkeeran" filed a lawsuit against the government authorities who were interfering with the rights of the publishers to publish the autobiography. The court allowed the editor's writ petition. During the whole of the case's handling. Regardless of whether the publishing is based on erroneous facts or assumptions, the Supreme Court of the United States determined in a judgment that will go down in history that public servants do not have a right to privacy when it comes to topics that relate to their public duty. As a result of this lawsuit, it was determined that the government does not have the legal authority to deny the publication of defamatory words in the past. As soon as it is shown that the publishing is not accurate, the authorities will be able to take the necessary actions. A person's right to life and personal liberty, which includes the right to privacy, is guaranteed under Article 21 of the Constitution of India. On the other hand, the right to privacy of an individual is not an unconditional right in India. There are a number of restrictions, including the following: adhering to a legal procedure that is

just, fair, and reasonable; serving the interests of India's sovereignty and integrity; being in the best interest of the state; not being available to individuals who voluntarily enter into controversy; and being against the interests of private citizens.

OBJECTIVE

1. To examine how India's right to privacy is affected by data breaches and digital surveillance.
2. To assess current data protection legislation and identify the main legal obstacles to protecting privacy in the digital era.

METHODOLOGY

An approach to doctrinal legal research is used in this work, which focuses on the examination of constitutional provisions, historic judgments, legislation, and legal recommendations. In addition to this, it employs a comparative legal research methodology to investigate the most effective techniques that are used in other countries, such as the United States of America, the European Union, and the United Kingdom. In order to have an understanding of the evolving nature of the right to privacy, it is necessary to perform a critical study of secondary sources. These secondary sources include scholarly publications, reports from law commissions, and policy papers from the government.

CONCEPTUAL FRAMEWORK OF THE RIGHT TO PRIVACY

Definition And Dimensions of Privacy

Beyond the fundamental right to be alone, the concept of privacy encompasses a number of other aspects and perspectives. Alan Westin provided a definition of the phrase, which he described as the "claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others." It is possible that this ground-breaking revelation is where contemporary privacy law may trace its origins back to. Rather of focusing on a single identified interest, Daniel J. Solove (2006) expanded the scope of the investigation to include a complex network of interconnected dangers to privacy. These threats include monitoring, data processing, and dissemination. The ability to make one's own judgments, the protection of one's own integrity, and the management of one's own data are all aspects that fall under the umbrella of the right to privacy, which is an essential component of human dignity and liberty.

Evolution Of the Right to Privacy in India

In India, there has been a gradual but consistent movement toward the constitutional protection of individuals' right to privacy. The Supreme Court of India made history by denying the right to privacy as an essential right in the case of *Kharak Singh v. State of Uttar Pradesh*, which was the first time the court adopted a restricted viewpoint. Ultimately, this position was overturned by the Supreme Court's decision to recognize a penumbral right to privacy under Article 21. This decision was most famously made in the case of *Gobind v. State of Madhya Pradesh*. The verdict that was made by a panel of nine judges in the historic case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* was unanimous. The panel declared that the right to privacy is inextricably linked to the right to life and personal liberty, as mentioned in

Article 21 of the Indian Constitution. The case was a pivotal point in the interpretation of the Constitution because it upheld the concept of privacy as a multifaceted right that incorporates autonomy, dignity, and physical integrity.

International Human Rights Standards on Privacy (UDHR, ICCPR, ECHR)

From the beginning of time till the present day, the fundamental nature of the right to privacy has been protected in accordance with international human rights standards. Every individual has the right to be free from the arbitrary invasion of their privacy, family life, place of residence, or private communication, as stated in Article 12 of the Universal Declaration of Human Rights, which was adopted in 1948. According to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which was established in 1966, individuals have the right to defend their honor and reputation against assaults that are contrary to the law. Article 8 of the European Convention on Human Rights guarantees the right to privacy, the right to one's own house, and the freedom to communicate. In a broad sense, the European Court of Human Rights has understood this right to include protection against the collection of biometric information, monitoring of such information, and the use of data. In accordance with these international principles, the respect for personal space is an essential component of human dignity and the active citizenship of individuals.

Distinction Between Informational, Bodily, And Spatial Privacy

Informational privacy, physiological privacy, and geographical privacy are the three main forms of privacy that most people are familiar with. The capacity to exercise control over the transmission of one's personal information is what is meant by the term "informational privacy." Especially in this digital age, when the dangers posed by technology that gather and monitor data are at an all-time high, this is of the utmost importance. The significance of bodily privacy is brought to light by cases such as *Suchita Srivastava v. Chandigarh Administration* (2009). This right encompasses the right to make one's own decisions about one's own body, especially those decisions that pertain to fertility, health, and physical integrity. The term "spatial privacy" refers to the right of a person to live in peace inside their own home or place of work, free from unwelcome physical and technological intrusions. This right is referred to as the "right to live in peace." It is essential to take into consideration these basic and interconnected characteristics in order to acknowledge privacy as a comprehensive right rather than a collection of individual rights.

TECHNOLOGICAL INTRUSIONS AND EMERGING CHALLENGES

Surveillance Technologies (CCTV, Facial Recognition, Drones)

The proliferation of technologies such as closed-circuit television (CCTV), facial recognition systems (FRS), and drones has resulted in the continual surveillance of a great number of public and private spaces. There are valid concerns over the absence of appropriate legal frameworks for mass surveillance in India, especially in locations such as Hyderabad and Delhi, which are among the most surveyed cities on a global scale. The lack of a consent-based approach, high error rates (especially among disadvantaged groups), and the prospect of exploitation by state actors are some of the most significant concerns that have been raised against face recognition technologies. In spite of the fact that the Supreme Court acknowledged in

Puttaswamy that surveillance must fulfill the standards of legality, necessity, and proportionality, face recognition and drone monitoring often flout these basic principles with impunity.

Data Mining, Social Media, And Big Data Analytics

The proliferation of personal data that is produced online has increased with the advent of platforms that are part of the Web 2.0 ecosystem. Websites that facilitate social networking collect vast amounts of personal information from their users by means of their cookie policies and terms of service, which are sometimes shrouded in mystery. Because of the Cambridge Analytica scandal, businesses and governments have the ability to employ data mining and big data analytics to develop profiles of individuals, make predictions about the conduct of those individuals, and even influence the choices that are made about policy. Because there are no rules in place that effectively safeguard user data, there is an even larger risk of user data being commodified. Not only does this phenomenon put democratic debate and individual liberty in jeopardy, but it also puts the privacy of people's personal information at risk.

Artificial Intelligence and Predictive Algorithms

As a result of the development of artificial intelligence (AI), there has been a paradigm shift taking place in the processing and use of personal data. The operations of automated recruitment tools, credit scoring systems, and algorithms that forecast police conduct are not transparent, and these systems often contain biases and blunders. Additionally, there is a lack of openness in the operations of these systems. By utilizing information that may not have been acquired with permission or adequately anonymized, these algorithms are able to make significant judgments, which is in direct opposition to the principles of openness and fairness. As a result of concerns over the use of artificial intelligence (AI) to monitor social programs and law enforcement in India, the urgent need for ethical principles and legal safeguards has been brought to light.

Cybersecurity And Data Breaches

In recent years, there has been an increase in the number of data breaches that involve significant corporations. These breaches usually include banks, websites belonging to the government, and healthcare institutions. The Computer Emergency Response Team (CERT-IN) (2021) reports that India saw more than 1.16 million cybersecurity incidents in the year 2020. This kind of data breach puts people's identities at danger of being stolen, in addition to causing them to suffer financial loss and harm to their reputations. In spite of the fact that the Digital Personal Data Protection Act, 2023 was approved, there is still a dearth of enforcement measures, and the penalties are sometimes insufficient to deter reckless behavior. In addition to individual data protection rights, a comprehensive cybersecurity architecture is required in order to ensure the preservation of informational privacy in the world of digital technology.

Role Of Private Tech Giants in Data Harvesting

Multinational information technology companies like as Meta, Google, and Amazon have access to customer data that is unrivaled because of their widespread presence in a variety of online ecosystems. These ecosystems include search engines, social media, e-commerce, and smart gadgets. The surveillance capitalism model, which tracks every move of customers in order to customize adverts and influence their

preferences, has been the foundation around which these businesses have built their company operations. Due to the lack of data localization and clarity about jurisdiction, these corporations are able to sidestep the domestic privacy standards that are in place. Due to the absence of robust regulatory oversight, internet firms in India have been able to benefit from user data with little to no accountability, which has led to the emergence of digital colonialism and consent-based data governance. These concerns have developed as a result of the fact that internet companies have been able to profit from user data.

LEGAL FRAMEWORK GOVERNING PRIVACY IN INDIA

Constitutional Recognition Post-Puttaswamy (2017)

The case of Justice K.S. Puttaswamy (Retd.) v. Union of India, which was determined by the Supreme Court, is considered to be a landmark decision in the field of Indian privacy legislation. As a component of the rights to life and personal liberty, the right to privacy is a fundamental right under Article 21 of the Constitution, according to the decision that was reached unanimously by the nine judges who made up the panel representing the Constitution. The Supreme Court stressed that various rights are included in the concept of privacy. These protections include the freedom to make one's own judgments, the ability to manage one's own information, and the freedom to keep one's physical integrity. Drawing on precedents established by international law authorities such as the European Court of Human Rights and the Canadian Charter, it established the three-pronged test of legitimacy, necessity, and proportionality for any government intrusion into the right to privacy. This test was necessary for every government intrusion into the right to private. The right, on the other hand, was mostly idealistic at that time period since there was no real privacy law in place.

The Information Technology Act, 2000 And Its Amendments

When it comes to matters concerning information technology and electronic data, the Information Technology Act, 2000 (IT Act) is the primary legislation that governs India. You have the right to seek compensation under Sections 43A and 72A of the Act in the event that a third party discloses your personal information without your consent or displays carelessness with regard to your personal information. The inadequacy of existing policies in resolving privacy concerns in digital realms is due to the fact that they are limited in scope and do not provide full safeguards. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Section 43A), which exclusively apply to corporate entities, primarily insulate state actors from responsibility when it comes to the protection of sensitive personal data or information. In addition, the Act's penalties are not very severe, and its enforcement has been uneven, which makes it difficult to detect and prevent substantial infractions.

The Personal Data Protection Bill, 2019 (Now DPDP Act, 2023) – Analysis and Gaps

The Digital Personal Data Protection Act, 2023 (DPDP Act) was introduced by the Indian government in order to set laws for the management of personal information. This was done after long talks and the report that was produced by the Justice B.N. Srikrishna Committee in 2018. There is a degree of conformity between the Act and worldwide standards such as the General Data Protection Regulation (GDPR). The Act encompasses concepts such as data principals, consent-based processing, and data fiduciaries. Nevertheless, it has been subject to criticism for purportedly undermining the concepts of purpose

limitation and proportionality by enabling government bodies to avoid legal examination via the use of ambiguous assertions of national interest. For a number of reasons, including the absence of a robust and impartial data protection authority and the restricted user redressal methods, the implementation structure is fundamentally inadequate.

Sectoral Regulations: Uidai (Aadhaar), Rbi Guidelines, Telecommunication Laws

Rather than being governed by broad legislation, personal privacy in India is governed by sector-specific regulations. Concerns have been raised by a few individuals over the possibility that the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 might facilitate the collecting of data in a centralized manner and the surveillance of a large number of individuals. It is permissible under the law to utilize demographic and biometric information for the purpose of identification. In spite of the fact that the Aadhaar ruling (2018) established that Aadhaar is constitutional, the court has limited its use to social programs and PAN-linking. This makes it difficult for commercial companies to be forced to adopt Aadhaar. As of right now, operators of payment systems are obligated to comply with the data localization rules that were imposed by the RBI. Regulatory law pertaining to telecommunications requires the storage of metadata, which has given rise to concerns over passive surveillance and the possibility of privacy being violated. On the other hand, rules are disjointed, and the privacy of users is not effectively safeguarded since there is no coordinated oversight across a wide range of sectoral legislation.

JUDICIAL TRENDS AND KEY CASE LAWS

Kharak Singh V. State Of Uttar Pradesh (1963)

In the case of Kharak Singh v. State of Uttar Pradesh, which featured the challenge to police surveillance tactics under the Uttar Pradesh Police Regulations, the right to privacy was introduced into the Indian constitutional conflict. This case focused on the constitutionality of the state of Uttar Pradesh. An overwhelming majority of the Supreme Court's judges came to the conclusion that the right to personal privacy is not a basic right since the Constitution does not guarantee it. In a crucial dissenting opinion, Justice Subba Rao claimed that breaking and entering someone's house constituted a violation of their "ordered liberty" as described in Article 21. This judgment was considered to be a landmark in the legal system. Despite the fact that it was not acknowledged at the time, this disagreement was significant in establishing the foundation for later privacy jurisprudence.

Govind V. State Of Madhya Pradesh (1975)

When it came to the case of Govind v. State of Madhya Pradesh, the Supreme Court used a more complex approach. The Supreme Court did highlight that privacy is a fundamental right that may be inferred from Articles 19(1)(d) and 21, despite the fact that these articles do not explicitly identify privacy as a fundamental right. In the event that there is a compelling public interest, Justice Matthew believes that there may be instances in which the right to privacy is not absolutely guaranteed. This ruling served as a signal for the commencement of a middle ground strategy that maintained the privacy of people while at the same time allowed for appropriate constraints.

Justice K.S. Puttaswamy V. Union of India (2017)

When the Supreme Court of India unanimously recognized the right to privacy as a fundamental right, which originated from Part III of the Constitution and was incorporated in Article 21, the landmark decision of Justice K.S. Puttaswamy v. Union of India⁴¹ reshaped Indian constitutional law. This recognition altered the landscape of Indian constitutional law. The author of the primary judgment, Justice D.Y. Chandrachud, said that the concept of privacy comprises the ability to make one's own choices, the autonomy over one's own body, and the right to determine one's own information. The choice of the Supreme Court to employ the three-pronged analysis of proportionality, need, and legality was significantly influenced by the case law that was established within the international community. By categorically rejecting previous rulings in the case of M.P. Sharma and the Kharak Singh majority opinion, the court firmly established the right to privacy as a basic right.

Aadhaar Judgment (2018)

The Supreme Court's ruling in K.S. Puttaswamy v. Union of India (Aadhaar) upheld the constitutionality of the Aadhaar program within the constraints imposed by the case. In his majority ruling, Justice A.K. Sikri backed the Aadhaar design, arguing that privacy rights were safeguarded by data protection protections. In addition to stating that there should be a decrease in metadata storage requirements, the Supreme Court barred private organizations from accessing Aadhaar data. The decision was criticized by Khera (2019) for failing to include adequate safeguards and for weakening the proportionality test set down by Puttaswamy (2017).

Internet freedom foundation v. Union of India (2020)

In the case of Internet Freedom Foundation vs. Union of India, the petitioners disputed the implementation of the facial recognition system (FRS) on the grounds that state entities did not possess the required legal authorization. The continuing legal actions, which have not yet reached a conclusion, have brought to light the private issues that are associated with biometric monitoring as well as the need of enacting regulations that safeguard personal information. Through the application of the Puttaswamy paradigm, the petition makes the argument that the pervasive surveillance of the government without the appropriate power results in conditions that violate the Constitution. According to Ramanathan (2021), this developing trend demonstrates how civil society organizations are using constitutional remedies to demonstrate that governments have infringed the digital rights of their people.

COMPARATIVE ANALYSIS: GLOBAL PRIVACY FRAMEWORKS**General Data Protection Regulation (GDPR) – European Union**

When it comes to data regulation that protects personal information, the General Data Protection Regulation (GDPR) that was enacted by the European Union established the norm. 2018 marked the beginning of the implementation of this kind of privacy regulation. The General Data Protection Regulation (GDPR) is based on a framework that includes the following principles: lawfulness, justice, accountability, transparency, purpose restriction, data minimization, accuracy, storage limitation, and integrity. Under the General Data Protection Regulation (GDPR), users have a number of rights, including

the opportunity to access their personal data, rectify data inaccuracies, demand disclosure of their information, and request erasure of their data, which is often referred to as the "right to be forgotten." Additionally, data controllers are eligible for severe fines in the event that they fail to comply with regulations, and data protection impact assessments are required. Data processing and user permission are currently being approached in a different manner by companies all over the world as a result of the regulation's focus on privacy by default and design and its implementation. For instance, the General Data Protection Regulation (GDPR) is an example of a comprehensive data protection system that is driven by permission and that India can potentially adopt.

Usa's Sectoral Approach and Fourth Amendment Rights

On the other hand, the United States of America employs a sectoral model, which is in contrast to the omnibus method that is used by the European Union (EU), which oversees privacy via a patchwork of legislation such as GLBA, COPPA, and HIPAA. The Fourth Amendment, which forbids unreasonable searches and seizures, has been interpreted by the courts to give some safeguards for personal privacy, notably against governmental surveillance. Although the right to privacy is not directly mentioned in the Constitution of the United States of America, courts have interpreted it in an appropriate manner. This is despite the fact that the growth of corporate data collection technologies and surveillance operations such as PRISM have shown significant gaps in privacy protections. The rights of consumers vary from one state to the next, and the federal government does not have a collective agency that is responsible for protecting data. It is possible that India may get an understanding of the risks associated with sector-specific privacy legislation that are either weak or inconsistent as a result of this fractured approach.

Surveillance Reforms in The Uk and Canada

Both Canada and the United Kingdom have made major improvements to the privacy legislation frameworks that they have in place. In accordance with the Data Protection Act of 2018, the United Kingdom is responsible for carrying out the responsibilities outlined in the General Data Protection Regulation (GDPR). The Information Commissioner's Office (ICO) is in charge of exerting powerful supervisory powers over local enforcement. In the case of *Privacy International v. Investigatory Powers Tribunal*, the court system in the United Kingdom ruled against monitoring tactics that result in an undue infringement of individuals' right to privacy. In 2019, the Investigatory Powers Tribunal, after a landmark verdict in that case, placed mass surveillance under the supervision of the court system. Public sector organizations, such as the government of Canada, are expected to comply with the Privacy Act (1983) in combination with the Personal Information Protection and Electronic Documents Act (PIPEDA) in order to exercise control over the manner in which they collect and use personal data. In order to combat both artificial intelligence and facial recognition technologies, the Office of the Privacy Commissioner (OPC) is working to enact more rigorous privacy regulations. The enforcement frameworks of both countries recognize open, independent institutions that possess substantial regulatory authority. India is attempting to enhance the quality of its privacy laws, which is a characteristic that exists in both countries' frameworks.

Lessons India Can Learn

In terms of privacy management, India may learn useful lessons from the worldwide legislative frameworks that are now in place. As a result of the fact that the sector-by-sector regulation that is now in place in India is unclear, the nation needs a unified data protection law similar to the GDPR. The establishment of a data protection agency that had quasi-judicial powers and the ability to independently oversee operations is seen to be the most successful method for establishing public trust in compliance. Data minimization, purpose limitation, and user consent are all data protection criteria that the nation need to apply, especially for the activities of the government that deal with the processing of data. The legal system needs to provide a framework for the examination of surveillance measures, as well as for the protection of biometric data and material created by artificial intelligence via the implementation of institutional rules. In order for India to accomplish its digital revolution, it is necessary for the country to shift its data handling strategy from operational compliance to human rights protection under democratic oversight inside the country.

CONCLUSION

Alongside the expansion of other digital rights, the right to privacy online has become more significant for democracies such as India today. Despite the fact that the constitutional recognition of privacy as a fundamental right has provided a firm foundation, the enforcement of this right is nevertheless challenged by challenges such as the frequent breach of data, the lack of adequate measures, and the expanding risks posed by digital technology. There are impediments to their complete implementation, accountability, and international data governance, despite the fact that current law, such as the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023, makes substantial progress ahead. Increasing the public's awareness of digital rights, implementing technological safeguards, and implementing further legislative measures are all essential in order to ensure the safety of persons. The fundamental challenge that will continue to be faced in India in the process of developing a digital environment that is dependable and secure is the challenge of finding a balance between the expansion of technology, the growth of the economy, and the protection of personal privacy.

REFERENCES

1. Austin, G. (2001). *Working a Democratic Constitution: The Indian Experience*. Oxford University Press.
2. Banerjee, S. (2022). Surveillance and the State in India: The Growing Use of Facial Recognition. *Economic and Political Weekly*, 57(2), 15–18.
3. Banisar, D. (2011). *Speaking of Surveillance: The Need for Privacy Laws in India*. Privacy International.
4. Balkin, J. M. (2014). Digital speech and democratic culture: A theory of freedom of expression for the information society. *NYU Law Review*, 79(1), 1–58.
5. Basheer, S. (2015). India's Tryst with Data Privacy. *Indian Journal of Law and Technology*, 11(1), 1–18.
6. Bennett, Colin J. and Raab, Charles D., *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edition, MIT Press, Cambridge, MA (2006)

7. Bhatia, G. (2018). *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins India.
8. Bhatia, G. (2020). State Surveillance and the Right to Privacy in India. *NUJS Law Review*, 13(2), 1–26.
9. Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada.
10. Chandrachud, D. Y. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India. Supreme Court of India, W.P. (Civil) No. 494 of 2012.
11. Cate, F. H. (2010). The failure of fair information practice principles. In R. Gellman & P. Dixon (Eds.), *Privacy, due process and the computational turn*. Routledge.
12. Crawford, K., & Paglen, T. (2019). *Excavating AI: The politics of images in machine learning training sets*. AI Now Institute.
13. de Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70.
14. Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
15. Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown Law, Center on Privacy & Technology.
16. Govind vs. State of Madhya Pradesh, 1955 CrLJ 1275; Govind vs. State of Madhya Pradesh, AIR 1975 SC 1378
17. Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 165, 10–13.
18. Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
19. Helfer, L. R., & Slaughter, A. M. (1997). Toward a theory of effective supranational adjudication. *The Yale Law Journal*, 107(2), 273–391.
20. Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59.
21. Justice K.S. Puttaswamy vs. Union of India, 2017 10 SCC1