CHANAKYA LAW REVIEW (CLR)

VOL. V (ISSUE 01) JAN-JUNE 2024, pp. 66-86

DIGITAL SURVEILLANCE AND CIVIL RIGHTS: ASSESSING THE IMPACT ON PRIVACY

Dr. Rumi Dhar[1]
Ms. Sonia Nath[2]

ABSTRACT

In an age characterized by swift technological progress and rapidly increasing security challenges, the surveillance landscape in India has experienced substantial transformation. The importance of safeguarding national security has led to the implementation of various surveillance laws; however, there is no specific legislation to govern surveillance in India, but the Information Technology Act of 2000 and the Indian Telegraph Act of 1885 are used to regulate surveillance. Laws pertaining to surveillance have been a subject of ongoing discussion, especially concerning the delicate balance between national security imperative and preserving the rights to privacy of individuals. The issue has become even more pressing in the digital age, where various government agencies and private companies collect and store enormous volumes of personal data. Addressing these concerns, India has recently passed the Digital Personal Data Protection Act 2023, which seeks to find an equilibrium between national security considerations and the safeguarding of individual privacy rights. Surveillance is a tool for maintaining the nation's sovereignty, unity, and integrity. Now, the question arises whether surveillance by the government violates the individual's right to privacy. The objective of the paper is to conduct a thorough analysis of the current laws and regulations pertaining to surveillance in India, evaluating their implications for the rights and liberties of individuals.

KEYWORDS: *Right to Privacy, Digital Surveillance, Data Protection, and Digital Personal Data Protection Act 2023.*

[1] Assistant Professor, Department of Law, Nagaland University (a Central University) Nagaland, India, Email: rumidhar@nagalanduniversity.ac.in.
[2] Research Scholar, Department of Law, Nagaland University (a Central University) Nagaland, India, Email: sonia_rs2022@nagalanduniversity.ac.in.

INTRODUCTION

In today's first-running technological world, the internet has become essential to our life. Every individual in society needs some space in the digital world[3]. The internet has not only made people addicted to digital life, but they are also getting more vulnerable to cybercrime. Technology advancements have fastened our communication, transportation, and even the method of executing trans-border crimes, such as cybercrimes[4]. Cybercriminals or hackers who know how to misuse cyberspace are not only playing with the privacy of individuals but also misusing cyberspace, creating a risk to national security. Over the recent years, India has experienced notable technological advancements that have led to improved surveillance capabilities. However, the growth of these capabilities has led to growing concerns about the impact on individual privacy rights. Surveillance is a critical tool for national security agencies to control criminal activities and terrorist threats[5]. Though these measures are essential for maintaining national security, they also raise significant concerns about the potential abuse of surveillance powers and the erosion of individual privacy rights.

In tackling these concerns, it is crucial for India to find a sophisticated equilibrium between national security and the safeguarding of privacy rights. This can be accomplished through robust oversight and accountability measures, ensuring that surveillance powers are wielded in a lawful and proportionate manner. Balancing the need for national security with the protection of individual liberties is a complex and challenging task for lawmakers in India. The Indian government has enacted numerous laws and policies to address diverse threats to national security, encompassing terrorism, cyber-attacks, and organized crime. These laws have granted the government and law enforcement agencies broad surveillance powers, including the interception and monitoring of electronic communications, surveillance of public spaces, and the collection of personal data[6].

The enactment of the Digital Personal Data Protection Act 2023 marks a substantial stride in securing the privacy of Indian citizens within the digital domain. This Act acknowledges the significance of safeguarding personal data and sets forth a structure for collecting, storing, processing, and sharing such information. It outlines individuals' rights regarding their personal data and imposes strict penalties for any unauthorized access, utilization or disclosure of such information.

---

[3] Tehilla Shwartz Altshuler, "Privacy in a digital world", Join TechCrunch+, Sept 27th, 2019, (https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world/) (accessed June 5th, 2024).

[4] UTICA University, "Ten Ways Evolving Technology Affects Cybersecurity", April 30, 2020, (https://programs.online.utica.edu/resources/article/ten-ways-evolving-technology-affects-cybersecurity) (accessed June 8, 2024).

[5] Maria Xynou, "Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles", (https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf) (accessed June 12, 2024).

[6] Kamesh Shekar and Shefali Mehta, "The State of Surveillance in India: National Security at the Cost of Privacy", Observer Research Foundation (ORF) Feb 22, 2022, (https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india), (accessed June 07, 2024).

At the same time, Section 17(2)(a)[7] of the Act recognizes the legitimate need of the government to conduct surveillance for national security purposes. The law permits the legal interception of identifiable details under certain circumstances, including safeguarding India's security, fostering amicable relations with other nations, maintaining public order, and preventing the instigation of any recognizable offences. This reflects a considerate approach to reconciling national security considerations with individual privacy rights, recognizing the necessity for surveillance while imposing stringent restrictions and safeguards[8].

However, the Act is not without its critics. Some argue that the provisions for lawful interception are too broad and vaguely defined, potentially allowing for excessive government intrusion into individuals' privacy[9]. Furthermore, there are apprehensions regarding the effectiveness of enforcement mechanisms and the possibility of the misuse of authority in the gathering and utilizing of personal data for surveillance purposes. The paper explores the complex relationship between digital surveillance and civil rights, focusing on the impact of surveillance practices on privacy. Through a detailed analysis of legal framework, case studies and theoretical perspectives, this paper seeks to understand how digital surveillance is reshaping the landscape of civil liberties and exploring potential pathways for balancing security needs with the protection of individual rights.

RIGHT TO PRIVACY IN THE DIGITAL AGE

The contemporary era is witnessing a continual evolution in the concept of the right to privacy. The swift progress of technology and the growing reliance on digital platforms for communication and information sharing have elevated privacy rights to a significant and concerning issue. Additionally, with the advancement of technology, our data is getting more exposed to the public domain. As a result, our data often gets compromised without consent. Development requires new thinking to redefine the traditional definition of the right to privacy. The post-Menka Gandhi[10] era has witnessed fascinating developments in Constitutional jurisprudence. The Supreme Court has extended the width of Article 21 by giving an extensive definition of life and liberty.

The right to privacy is a fundamental human right recognized by international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

[7] The Digital Personal Data Protection Act, 2023, s 17(2) The provisions of this Act shall not apply in respect of the processing of personal data-(a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offences relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it.

[8] Nishith Desai Associates, "India's Digital Personal Data Protection Act, 2023: History in the Making", Aug 7, 2023 (https://www.nishithdesai.com/NewsDetails/10703), (accessed June 5, 2024)

[9] Goyal Piyush, "7 major shortcomings of Digital Persona Data Protection Act, 2023", Medium Aug 17, 2023, (https://medium.com/@piyushgoyal2021/7-major-shortcomings-of-digital-personal-data-protection-act-2023-7ec16368332e), (accessed June 12, 2024).

[10] Maneka Gandhi v Union of India- AIR 198 SC 597; (1978) 1SCC 248.

Article 21[11] of the Indian Constitution ensures that "*No person shall be deprived of his life and personal liberty except according to procedure established by law*"[12]. Here, life does not mean only human life but a dignified life, including all aspects of complete and worthy living. The literal meaning of privacy is "*the of being alone, or the right to keep one's personal matters and relationship secret"*.**[13]** In today's world, privacy is not only confined to the physical but also to the virtual.

Article 12 of the Universal Declaration of Human Rights***[14]*** ensures that

> **"*No one shall be subjected to arbitrator interference with his privacy, family home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such inference or attacks*"**[15].

Further, Article 17 of the International Covenant on Civil and Political Rights***[16]*** guarantees

> ***"(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks"***[17].

The right to privacy encompasses the freedom from unwarranted government surveillance of any individual. In December 2018, the Ministry of Home Affairs (Cyber and Information Security Division) circulated a Gazette notification delegating its power to ten (10) organizations to monitor the inception of any messages, decrypting of any information generated, transmitted from a source, received, or stored in any computer resource[18]. The right to life has encountered new dimensions and complexities in the digital age. The rapid progress of technology and the widespread adoption of digital platforms have broadened the scope of the right to life, encompassing physical well-being and safeguarding an individual's personal identity, dignity, and data privacy in the digital domain.

Growth of Right to Privacy in India

[11] The Constitution of India, art 21- Protection of life and personal liberty, Bakshi P M, *The Constitution of India* 74 (Universal Publication, 17th Edition 2021).
[12] Ibid
[13] Cambridge Dictionary, (https://dictionary.canbridge.org/dictionary/english/privacy)
[14]Universal Declaration of Human Rights, UN General Assembly Dec 10, 1948, (https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf).
[15] Universal Declaration of Human Rights 1948, art 12, (https://www.un.org/en/about-us/universal-declaration-of-human-rights)
[16] International Covenant on Civil and Political Rights, General Assembly Resolution 2200A(XXI), Dec 16, 1966, (https://www.ohchr.org/sites/default/files/ccpr.pdf).
[17] International Covenant on Civil and Political Rights 1966, art 17 (https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights)
[18] Ministry of Home Affairs (Cyber and Information Security Division) Gazette notification number S.O 6227(E.) Dec 20th, 2018, (https://www.humanrightsinitiative.org/download/MHA-SO6227-Dec18.pdf), (accessed June 3, 2024).

In India, the right to life is enshrined in Article 21 of the Constitution, which guarantees the right to life and personal liberty. Over the years, the Indian judiciary has broadly interpreted this right, encompassing various aspects of an individual's life, including the right to privacy and data protection[19]. The development of the right to privacy can be acknowledged through case laws:

1954 ⇨ ***M P Sharma v Satish Chandra[20]***

The Supreme Court, in discussing the search and seizure of a document, ruled that the right to privacy, as per the Indian Constitution, does not qualify as a fundamental right.

1963 ⇨ ***Kharak Singh v State of UP and Ors.*** [21]

The Supreme Court determined that the right to privacy is integral to the right to life and personal liberty. The surveillance by police was challenged and led to the Supreme Court expanding the right to life to encompass a new aspect, namely personal freedom.

1963 ⇨ ***Govind v State of Madhya Pradesh and others[22]***

For the first time, the right to privacy under personal liberty was recognized. The court held the existence of privacy under Article 21 of the Indian Constitution.

1973 ⇨ ***R M Malkani v State of Maharashtra[23]***

The Supreme Court observed that it would not allow the protection of citizens to be threatened by allowing law enforcement to use unlawful or irregular methods.

1978 ⇨ ***Smt Menka Gandhi v Union of India & Anr[24]***

The Supreme Court widened the ambit of Article 21 and held that personal liberty covers a variety of rights, and some have the status of fundamental rights under Article 19

[19] Thaorey Payel, "Legal Introspection Towards the Development of Right to Privacy as Fundamental Right in India", Indonesian Law Review, Dec 31, 2021, Volume 11 No. 3, (https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1238&context=ilrev) (accessed June 16, 2024).
[20] M P Sharma v Satish Chandra AIR 1954 SCR 1077.
[21] Kharak Singh v State of UP and Ors AIR 1963 SC 1295.
[22] Govind v State of Madhya Pradesh and others 1975(2) SSC 14.
[23] R M Malkani v State of Maharashtra AIR 1973 SC 157.
[24] Smt Menka Gandhi v Union of India & Anr AIR 1978 SC 597.

1995 ⇨ ***R Rajgopal v State of TN***[25]

The Apex Court held that no one could publish anything without consent. If he does so, he would violate that person's right to privacy and be liable for damages (Right to let alone).

1999 ⇨ ***Mr. X v Hospital "Z"***[26]

The Court held that when there is any conflict between two fundamental rights, including the right to privacy. Then, the right to further public morality or the public interest will prevail.

2005 ⇨ ***District Registrar and Collector v Canara Bank***[27]

It was held that it is right to let alone, and every citizen has the right to safeguard his privacy.

2010 ⇨ ***Naz Foundation v Govt of NCT of Delhi (2009[28])***

The Delhi High Court in the judgment regarding consensual homosexuality under Section 377 of the Indian Penal Code, the Delhi High Court ruled that Section 377 contravenes Articles 14, 15, and 21 of the Indian Constitution. Sec 377 causes unreasonable discrimination, describing homosexuals as a class and criminalizing their consensual sex. No person can enjoy life without dignity and privacy.

2010 ⇨ ***Selvi and Others v State of Karnataka[29]***

The Supreme Court sheds light on mental privacy in and acknowledges the difference between physical and mental privacy. The compulsory administration of neuroscientific investigative techniques violates the rights of the accused.

.

2018 ⇨ ***Navjet Singh Johar v Union of India (2018)***[30]

This case revisited the issue of section 377 of the IPC, which criminalized homosexual acts. The Supreme Court, in a historic judgement, decriminalized consensual homosexual acts between adults, affirming the right to privacy, dignity, and equality. The Court emphasized that sexual orientation is an essential attribute of privacy and that the state has no business interfering in the intimate affairs of individuals.

[25] R Rajgopal v State of TN 1995 SC 264.
[26] Mr. X v Hospital "Z AIR 1999 SC 495.
[27] District Registrar and Collector v Canara Bank AIR 2005 SC 186.
[28] Naz Foundation v Govt of NCT of Delhi 2010 CRI L J 94
[29] Selvi and Others v State of Karnataka (2010) 7 SCC 263.
[30] Navjet Singh Johar v Union of India AIR 2018 SC 4321.

Joseph Sine v Union of India (2018[31])

The Supreme Court stuck down section 497 of IPC, which criminalized adultery. The court ruled that the law was archaic and violated the right to privacy and equality.

The evolution of the right to privacy in India reflects the judiciary's responses to the challenges posed by technological advancements, societal changes, and the need to protect individual freedoms. From its initial reluctance to recognize privacy as a fundamental right, the Indian judiciary has gradually expanded the scope of privacy, culminating in its recognition as a constitutionally guaranteed right.

Recent Development in the Right to Privacy

India has witnessed significant progress in technology and surveillance capabilities in recent years. Nevertheless, expanding these capabilities has raised increasing concerns regarding its implications on individual privacy rights. In the case of ***Justice Puttaswamy (Retd) v Union of India and Ors,***[32] the Supreme Court established a more reformed and well-established law regarding privacy. It has reaffirmed the right to privacy as a fundamental right, an essential aspect of Article 21 of the Constitution of India.

The emergence of the digital age has introduced new complexities in the form of cybercrime, data breaches, and violations of online privacy rights. In response, the Indian government has taken significant measures to tackle these challenges and safeguard the right to life in the digital realm. The Supreme Court of India 2017 affirmed the right to privacy as a fundamental right, setting the stage for the introduction of robust data protection laws like the Digital Personal Data Protection Act of 2023. This legislation has played a pivotal role in reshaping the regulatory landscape governing surveillance practices, serving as a crucial mechanism to balance the competing interests of national security and privacy rights. Its primary aim is to regulate the processing of personal data and empower individuals with increased control over their digital information. Later, the Supreme Court, in its recent judgement in the ***Anuradha Basin v Union of India,***[33] held that internet access had become an integral part of everyday life; therefore, freedom of speech and online expression are fundamental rights granted under Part III of the Indian Constitution.

Data Privacy

Data privacy is a fundamental human right that is essential to the functioning of a free and democratic

[31] Joseph Shine v Union of India AIR 2018 SC 4898
[32] Justice Puttaswamy (Retd) v Union of India and Ors AIR 2017 SC 4161.
[33] Anuradha Basin v Union of India 2019 SCC Online SC 1725.

society. It encompasses the right of individuals to control their personal information and to have it protected from unauthorized access, use, and disclosure. Personal data is constantly being collected and processed by a wide range of entities. One of the main challenges in the realm of data privacy is the ever-increasing amount of data being collected. With the proliferation of digital devices and the rise of the Internet of Things, we are constantly generating and sharing data without even realizing it. This includes our online activities, social media interactions, location data, and more. As a result, there is a growing concern about the potential for this data to be misused, whether it is through identity theft, unauthorized surveillance, or targeted advertising.

There has been a growing push for stronger data privacy laws and regulations in response to these challenges. In the European Union, the ***General Data Protection Regulation***[34] (GDPR) has set a benchmark for data protection regulations, providing individuals with more control over their personal data and placing greater obligations on businesses to protect this information. Similarly, the ***California Consumer Privacy Act***[35] (CCPA) In the United States, new requirements have been introduced for businesses to disclose their data collection practices and give individuals the right to opt out of the sale of their personal information. The ***Personal Information Protection and Electronic Documents Act***[36] of Canada applies to businesses engaged in commercial activity across provinces, and the ***Digital Personal Data Protection Act 2023***, comprehensive data protection legislation of India, aims to regulate the processing of personal data by businesses and enhance the rights of individuals.

Right to Be Forgotten

The right to be forgotten, also known as the right to erasure[37], is a concept that has gained significant attention with the implementation of the ***General Data Protection Regulation (GDPR)***[38] by the European Union (EU) in 2018. This entitlement enables individuals to demand the deletion of their personal data from online platforms and databases unless there is a valid justification for its retention. This right is intended to empower individuals with authority over their personal information and safeguard their privacy in the era of digital technology. In the age of digitization, the right to be forgotten undertakes a crucial role as personal data undergoes continuous collection, sharing, and utilization for various purposes. This right empowers individuals to safeguard their privacy and ensure that their personal information is not used in ways without

[34] EU General Data Protection Regulation 201/679 of the OJL 119, (https://gdpr-info.eu/).

[35] California Consumer Privacy Act of 2018, California Civil Code [1798.100-1798.199.100], https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[36] The Personal Information Protection and Electronic Documents Act, S.C 2000, c 5, Assented to 2000-04-13 (https://laws-lois.justice.gc.ca/eng/acts/p-8.6/).

[37] GDPR Right to be Forgotten- The right to be forgotten derives from the case Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez (C-131/12) (2014). For the first time, the right to be forgotten is codified and to be found in the General Data Protection Regulation (GDPR) in addition to the right to erasure. (https://gdpr-info.eu/issues/right-to-be-forgotten/).

[38] The European Union General Data Protection Regulation (EU) 2016/679, 27 April 2016, OJL 119/1 (EU), (https://gdpr-info.eu/).

their consent. Although the right to be forgotten is not explicitly defined in Indian law, it pertains to the capacity to eliminate particular information from public visibility, the internet, or any other public platform. This right, also known as the right to erasure, was brought forth by the EU GDPR.

The right to be forgotten is not an absolute right, there are limitations to this right under the GDPR. Article 17(1)[39] of the EU GDPR deals with the provisions relating to the right to erasure (right to be forgotten). Grounds under which the right to erasure can be exercised are:

1. Personal data becomes obsolete when it is no longer required for the original purpose for which it was collected or processed.

2. Revoking consent for processing, with no alternative legal grounds for data processing.

3. There are no compelling and justifiable reasons to persist with the processing.

4. Oppose the processing when personal data is being used for direct marketing.

5. Personal data has been handled unlawfully.

6. Erasing personal data is necessary to adhere to a legal obligation.

7. Personal data has been gathered concerning the provision of information society services.

While the legal framework in India does not formally acknowledge the right to be forgotten, but the judgements from different High Courts have recognized and affirmed this right in the absence of specific legislation in their respective judgements, such as in the case of ***Google India Pvt Ltd v Vishaka Industries and Ors,***[40] the Delhi High Court directed Google to de-index certain web pages that contain defamatory content. In the case of ***Dharamraj Bhanushankar Dave v State of Gujarat,***[41] the High Court refuses to acknowledge the right to be forgotten as there is no law in this matter, and hence no right has been violated.

[39] EU General Data Protection Regulation 201/679, art 17 - Right to erasure (right to be forgotten)- 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
(b)the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). *Supra* note 32.

[40] Google India Pvt Ltd v Vishaka Industries and Ors AIR 2020 SC 350.

[41] Dharamraj Bhanushankar Dave v State of Gujarat SCA 1854 of 2015.

In the case of ***Vasunathan v Registrar General***[42]**,** the Karnataka High Court recognizes the right to be forgotten, which involves enabling individuals to seek the deletion of their personal information or data from online platforms. In the ***Subranshu Rout @ Gugul v State of Orissa,***[43] the court concluded that the right to be forgotten in India would serve a critical role in safeguarding women's cyber interests[44]. In the case of ***Jorawer Singh Mundy v Union of India and Ors,***[45] the Delhi High Court directed Indiankanoon and Google to erase information about the petitioner. Thus, from the judgement of various High Courts, the courts acknowledge the right to be forgotten without legislation. A special leave petition was filed before the Supreme Court in the case of ***Karmanya Singh Sareen v Union of India***[46]**.** WhatsApp privacy breach case is where WhatsApp shares data with Facebook and all its companies for commercial and marketing advertisement purposes.

Furthermore, the proliferation of digital surveillance technologies has created a complex web of challenges for the protection of privacy rights in India. With the advent of advanced surveillance tools such as facial recognition technology, smart city surveillance systems, and biometric data collection, the scope of digital surveillance has expanded exponentially. This has raised concerns about the potential for mass surveillance and the erosion of individual privacy rights[47]. The recent debates over the implementation of the National Population Register (NPR) and the proposed use of biometric data for the surveillance of individuals have highlighted the need for comprehensive legal and regulatory frameworks to safeguard privacy rights in the digital age. The constant monitoring and tracking of individuals' online activities raises serious concerns about the right to privacy and personal data protection. The recent judgment by the Supreme Court of India in the landmark ***Justice K. S Puttaswamy (Retd) & Anr. Vs. Union of India & Ors***[48] case has established the groundwork for safeguarding privacy rights in the digital age. However, the challenges posed by digital surveillance continue to persist.

SURVEILLANCE LAWS IN INDIA

Surveillance means close observation or State of observation. Surveillance is a tool for the government to control crime in society and to have an eye on criminals. It is a precautionary step by the government to protect the State from external threats. In the present-day scenario, the government exercise surveillance

[42] Vasunathan v Registrar General 2017 SSC Online Kar 424.
[43] Subranshu Rout @ Gugul v State of Orissa BLAPL No. 4592 of 2020.
[44] Bang Yogesh (2021, July 19) Right to be forgotten: A tussle between data privacy and public information, The Daily Guardian, available at: https://thedailyguardian.com/right-to-be-forgotten-a-tussle-between-data-privacy-and-public-information/
[45] Jorawer Singh Mundy v Union of India and Ors WP (C) 3918/2020
[46] Karmanya Singh Sareen v Union of India SPL (C) No 000804/2017
[47] Shravistha Ajaykumar, "Ethical and Regulatory Considerations in the Collection and Use of Biometric Data", Observer Research Foundation (ORF) Oct 10, 2023, (https://www.orfonline.org/research/ethical-and-regulatory-considerations-in-the-collection) (acceded July 15, 2024).
[48] Justice K. S Puttaswamy (Retd) & Anr. Vs. Union of India & Ors (2017) 10 SCC 1, AIR 2017 SC 4161.

over email, telephonic conversation, CCTV surveillance, etc.[49] Surveillance laws in India have evolved in response to the challenges posed by technological advancements and the need for national security. These laws provide a legal framework for the use of surveillance technologies. Surveillance laws are aimed at protecting the country from internal and external threats, such as terrorism, espionage, and cyber-attacks. These laws grant the government and law enforcement agencies the power to gather information, monitor communications, and conduct surveillance on individuals and organizations that are deemed to be a threat to national security. While these laws aim to safeguard the nation and its citizens, they also raise significant concerns about the infringement of privacy rights.

In India, the regulation of surveillance is governed by various laws and regulations designed to balance national security concerns with the protection of the right to privacy. The primary legislative framework overseeing surveillance activities in the country is the ***Information Technology (Amendment) Act of 2008***[50], commonly known as the IT Act and the ***India Telegraph Act 1885***[51]. This legislation permits government agencies to intercept, monitor, and decrypt electronic communications under specific conditions, such as addressing threats to national security or conducting criminal investigations. There is no specific legislation in India for the surveillance of cyberspace. However, two legislations were there to regulate digital and telephonic surveillance:

1) Information Technology Act 2000 (for digital surveillance)
2) The India Telegraph Act 1885 (for telephonic surveillance)

Section 5[52] of the Indian Telegraph Act of 1885 grants authority to both the Central and State governments to intercept messages under certain conditions:

---

[49] Sangeeta Mahapatra, "Digital Surveillance and the Threat to Civil Liberties in India", German Institute for Global and Area Studies (GIGA) May 2021, No. 2, ISSN 1862-359X, (https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india) (accessed July 5th, 2024).

[50] The Information Technology (Amendment) Act, 2008 (Act no 10 of 2009), Gazette Notification Feb 5th, 2009, (https://www.indiacode.nic.in/bitstream/123456789/15386/1/it_amendment_act2008.pdf).

[51] The Indian Telegraph Act, 1885, (Act No. 13 of 1885), Gazette Notification July 22nd 1985, (https://www.indiacode.nic.in/bitstream/123456789/13115/1/indiantelegraphact_1885.pdf).

[52] The Indian Telegraph Act, 1885, s 5- Power of the Government to take possession of licensed telegraphs and to order interception of messages-

(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of an offence, for reason to be recorded in writing, by order, direct that any message or class of message to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by Government making the order or an officer thereof mentioned in the order; Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

(i) during an emergency or for public safety interests,

(ii) when deemed necessary, and

(iii) to uphold the sovereignty and integrity of the nation.

Likewise, section 69(1)[53] of the Information Technology Act of 2000 grants authority to both the Central and State Governments to intercept and decrypt any information that is transmitted, stored, or received in any computer source[54]. Recently, Google introduced an encrypted search facility. This encryption prevents computers from storing computer history and stops them from appearing in the AutoFill function for future searches. However, this encryption is not entirely private, as Google retains this information.

Government agencies in India are involved in surveillance, including the National Intelligence Grid (NIG), Crime and Criminal Tracking Network System (CCTNS), Central Monitoring System, Indian Computer Emergency Response Team (CERT-In), National Counter Terrorism Centre (NCTC), etc.[55]. India, the fastest developing country, must implement strong legislation and regulation policies to control cyberspace. National Intelligence Grid (NIG) Central Monitoring System (CMS) has been set up for surveillance on the internet, cell phone, private message as well as social media sites.

1) ***National Intelligence Grid (NIG):*** It links information saved in a server and network of a different department so that any department and intelligence agency can access it.

2) Crime and Criminal Tracking Network System (CCTNS): This network system helps store, analyze, transfer, and share data between various police stations and state headquarters.

3) Central Monitoring System: This system monitors every communication, including text messages, phone calls, online activity, social media conversations, content, etc.

[53] The Information Technology Act, 2000, s 69- Power to issue directions for interception or monitoring or decrypting of any information through any computer resources-
(1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section(2), for reason to be recorded in writing, by order, direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

[54] Saswat Singh, Surveillance in India Post the Right to Privacy Judgement, Legal Service India E-Journal, (https://www.legalserviceindia.com/legal/article-2273-surveillance-in-india-post-the-right-to-privacy-judgment.html), (accessed June 5, 2024).

[55] Maria Xynou and Elonnai Hickok, "Security, Surveillance and Data Sharing Scheme and Bodies in India", (https://cis-india.org/internet-governance/blog/security-surveillance-and-data-sharing.pdf) and Prashant Upadhay, " Surveillance in India and its Legality", Legal Service India.com, (https://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html) (accessed June 24, 2024).

4) The Indian Computer Emergency Response Team (CERT-In) is a nodal government agency for any computer security incident. It deals with cyber security incidents all over India.

5) The National Counter Terrorism Centre (NCTC) derives its power from the Unlawful Activities Prevention Act 1967. It was set up after the Mumbai 26/11 attack.

6) The National Cyber Coordination Centre (NCCC) screens all meta-data, ensuring better coordination between various intelligence agencies.

7) State cybercrime Coordinator and District Cybercrime cell.

8) Cyber Police Station.

India's growing legislative framework and policies are not strong enough to face future threats. Strong legislation is required to tackle cybercrimes and protect citizens' privacy. One of the drawbacks of the IT Act 2000 is that it needs to focus on cross-border cybercrime. India needs strong privacy and surveillance laws. The right to privacy and the necessity for surveillance consistently represent opposing aspects, creating conflict between citizens and law enforcement agencies.

3.1 *Information Technology Act 2000*[56]

The Information Technology (IT) Act in India is an extensive legal framework covering diverse aspects of electronic communication and data protection. A crucial component of the IT Act pertains to the government's authority for surveillance. The government can employ these surveillance powers based on specified conditions and procedures outlined in the Act. For instance, the government must obtain authorization from the competent authority before intercepting, monitoring, or decrypting any information. This authorization can only be issued under specific circumstances, such as when there is an imminent threat to national security or public order. Section 69[57] of the Act empowers the government to intercept, monitor, or decrypt any information created, transmitted, received, or stored in any computer resource when deemed necessary for the nation's sovereignty, integrity, defence, state security, diplomatic relations, public order, or the prevention of incitement to commit an offence. This provision's broad and ambiguous language gives the

[56] The Information Technology Act, 2000, (Act No. 21 of 2000), Gazette Notification June 9th, 2000, (https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf).

[57] The Information Technology Act, 2000, s 69-Power to issue directions for interception or monitoring or decrypting of any information through any computer resources-
(1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section(2), for reason to be recorded in writing, by order, direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. *Supra* note 54.

government extensive authority to surveil citizens and oversee their online actions. Section 69A[58] of the IT Act grants the government authority to restrict public access to any information via any computer resource when deemed essential for the interest of India's sovereignty, integrity, defence, state security, diplomatic relations, or public order. This provision enables the government to regulate and limit the dissemination of information on the Internet, thereby enhancing its surveillance capacities.

Section 69B[59] of the Act empowers the government to issue directives for the interception, monitoring, or decryption of any information via any computer resource if it is deemed necessary for investigating, preventing, or detecting any offence or ensuring cybersecurity. This provision allows the government to engage in surveillance for law enforcement purposes, enhancing its authority over digital communications. The clauses related to government surveillance powers in the IT Act of India are integral to electronic communication and data protection. While crucial for national security and public order, ensuring greater transparency, accountability, and oversight is imperative to prevent potential misuse.

3.2 *The Indian Telegraph Act 1885*[60]

The Indian Telegraph Act of 1885 is a legislative framework that governs the establishment, operation, and regulation of telegraph services in India. The Act contains several provisions that empower the government with surveillance powers to ensure national security and public order. One of the key provisions that empower the government with surveillance powers is Section 5(2)[61] of the Indian Telegraph Act, which states that the government or any officer authorized by the government may intercept or detain any message transmitted by telegraph. This provision gives the government the authority to monitor and intercept any

[58] The Information Technology Act, 2000, s 69A- "Power to issue directions for blocking for public access of any information through any computer resource- (1) Where the Central Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of any cognizable offences relating to above, it may subject to the provisions of sub-section(2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource. *Supra* note 54.

[59] The Information Technology Act, 2000, s 69B- Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contamination in the country, by notification in the Official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. (2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorized under sub-section (1), provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. *Supra* note 54.

[60] The Indian Telegraph Act, 1885, (Act No. 13 of 1885), Gazette Notification July 22nd, 1985, (https://www.indiacode.nic.in/bitstream/123456789/13115/1/indiantelegraphact_1885.pdf).

[61] The Indian Telegraph Act 1885 s 5(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of an offence, for reason to be recorded in writing, by order, direct that any message or class of message to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by Government making the order or an officer thereof mentioned in the order; Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained unless their transmission has been prohibited under this sub-section. *Supra* note 58.

telegraphic communication deemed necessary for the enforcement of public order or national security. This provision essentially grants the government the power to conduct surveillance on telegraphic communications and gather information as they see fit.

Surveillance laws in India are intricate and multi-dimensional, prompting significant considerations regarding the equilibrium between national security and individual privacy. Conversely, proponents of privacy contend that these laws frequently encroach upon citizens' fundamental rights and freedoms. The intricacy of India's surveillance laws lies in the participation of numerous government agencies in surveillance efforts. The absence of effective coordination and oversight among these agencies has resulted in a dearth of accountability and potential misuse. The complexity of surveillance laws in India is a result of a lack of clear and consistent regulations, a lack of oversight and accountability, and the rapid advancement of surveillance technology. This has created a situation where individual privacy rights are often compromised in the name of national security. Addressing these issues will require a comprehensive review and reform of India's surveillance laws to ensure that they strike the right balance between national security and individual privacy[62].

3.3 Judiciary on Digital Surveillance and Right To Privacy

The extensive adoption of surveillance technologies has posed a challenge to the conventional conception of privacy, prompting inquiries into the degree to which individuals can anticipate preserving their privacy in the digital era. Presently, the widespread deployment of surveillance technologies has brought forth crucial queries regarding the boundaries of government and corporate interference in the personal lives of individuals. Exploring surveillance's legal and ethical aspects is crucial to establish an equilibrium between security and privacy. The influence of surveillance on the right to privacy is deliberated, accompanied by references to pertinent case laws.:

Surveillance often involves monitoring individuals' activities, communications, and movements without their consent. This invasion of privacy can profoundly impact an individual's sense of autonomy and personal freedom. One of the significant cases that illustrates the impact of surveillance on the right to privacy is the case of ***Carpenter v. United States[63]***. In the present case, the United States Supreme Court deliberated on the legality of law enforcement agencies obtaining cell phone location data without a warrant, assessing whether it infringed upon the privacy rights protected by the Fourth Amendment. The Court concluded that such government acquisition of data constitutes a search under the Fourth Amendment and mandates the need for a warrant.

[62] Kamesh Shekar and Shefali Mehta, "The State of Surveillance in India: National Security at the Cost of Privacy", Observer Research Foundation (ORF) Feb 22, 2022, (https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india) (accessed July 07, 2024).

[63] Carpenter vs Unites States, 585 U.S. (2018).

Another relevant case that has implications for the right to privacy in the context of surveillance is the European Court of Human Rights judgment in ***Big Brother Watch and Others v. United Kingdom***[64] (2018). This case is centered on the lawfulness of government agencies engaging in the bulk interception of communications and sharing intelligence. The court determined that the expansive surveillance programs violate both the right to privacy and the right to freedom of expression, emphasizing the importance of implementing measures to prevent unwarranted intrusion into individuals' privacy. The judgement underscores the potential for surveillance to encroach upon fundamental rights and emphasizes the need for robust legal protection to safeguard privacy in light of technological advancements.

Another controversial case that sheds light on the impact of surveillance on the right to privacy is the case of Edward Snowden. In 2013, Edward Snowden, a former National Security Agency (NSA) contractor, leaked classified information about the NSA's mass surveillance programs. The leaked documents revealed the extent to which the NSA was collecting and analyzing data from millions of individuals, both within the United States and abroad, without their knowledge or consent. The Snowden case highlighted the potential for government surveillance to infringe upon the right to privacy on a massive scale. The surveillance activities revealed by Snowden went far beyond what most people would consider reasonable or proportionate, and they raised serious concerns about the impact of such surveillance on individual rights and freedoms[65].

The landmark judgment of ***Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017)*** marked the acknowledgement by the Supreme Court of India that the right to privacy is a fundamental right protected under the Indian Constitution. The Court upheld the triple test principle, which involves evaluating surveillance practices' legality, legitimate aim, and proportionality. This underscores the necessity for strict legal standards to be followed in surveillance measures, ensuring their suitability and necessity within the framework of a democratic society. The court asserted that a compelling state interest must warrant any infringement upon the right to privacy and must be executed in a lawful, equitable, and non-arbitrary manner. In the case of ***Internet Freedom Foundation vs Union of India***[66] (2019), The Internet Freedom Foundation, a digital liberties organization, filed a petition challenging the Indian government's surveillance program called the Central Monitoring System (CMS). The petition raised concerns about the surveillance process's lack of transparency and oversight.

DIGITAL PERSONAL DATA PROTECTION ACT 2023: A PARADIGM SHIFT

[64] Big Brother Watch and Others v United Kingdom, Application No. 58170/13.
[65] Kristain P Humble, "International Law, Surveillance and the Protection of Privacy", May 15, 2020, DOI: http://doi.org/10.1080/13642987.2020.1763315, (https://gala.gre.ac.uk/id/eprint/29181/1/29181%20HUMBLE_International_Law_Surveillance_and_the_Protection_of_Privacy_%28AAM%29_2020.pdf) (accessed June 16, 2024).
[66] Internet Freedom Foundation vs Union of India W.P.(C) No. 000044/2019.

The Digital Personal Data Protection Act of 2023[67] presents a critical juncture in the intersection of digital surveillance and data privacy. The increasing reliance on digital technologies in all aspects of modern life has brought unprecedented challenges to protecting personal information. On the one hand, digital surveillance is a necessary tool for law enforcement and national security, but on the other hand, it poses a significant threat to individual privacy. Thus, finding a balance between these competing interests is essential for the harmony and functionality of modern society. In response to these concerns, the Digital Personal Data Protection Act of 2023 represents a paradigm shift in the regulation of digital surveillance and the right to privacy. One of the Act's key provisions is Section 4[68], which outlines the principles of data protection. This section emphasizes the need for transparency and accountability in handling personal data. It requires organizations to obtain explicit consent from individuals before collecting or processing their personal data. Section 6(1)[69], which outlines the rights of individuals regarding their personal data. This section emphasizes the importance of informed consent and the right to access and control one's own data under section 11(1)[70]. This represents a significant departure from the previous approach to data protection, which often allowed for the indiscriminate collection and use of personal data without the knowledge or consent of the individuals concerned.

Additionally, Section 7(c)[71] of the act addresses the issue of digital surveillance. It stipulates that surveillance measures must be proportionate and necessary for legitimate purposes such as national security or public safety. This provision strikes a balance between the need for surveillance and the right to privacy, ensuring that surveillance activities are not arbitrary or excessive. Furthermore, Section 10(2)(a) of the act establishes the role of the ***Data Protection Officer[72] (DPO)***, who is responsible for supervising the execution and enforcement of the law. DPO plays a crucial role in ensuring entities comply with legal provisions and protect the rights of individuals.

---

[67] The Digital Personal Data Protection Act, 2023, (Act No. 22 of 2023), Gazette Notification August 11th, 2023, (https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf)

[68] The Digital Personal Data Protection Act, 2023, s 4(1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purposes, -
(a) for which the Data Principal has given her consent; or
(b) for certain legitimate uses.
(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law. *Supra* note 65.

[69] The Digital Personal Data Protection Act, 2023, s 6(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. *Supra* note 65.

[70] The Digital Personal Data Protection Act, 2023, s 11(1) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed. *Supra* note 65.

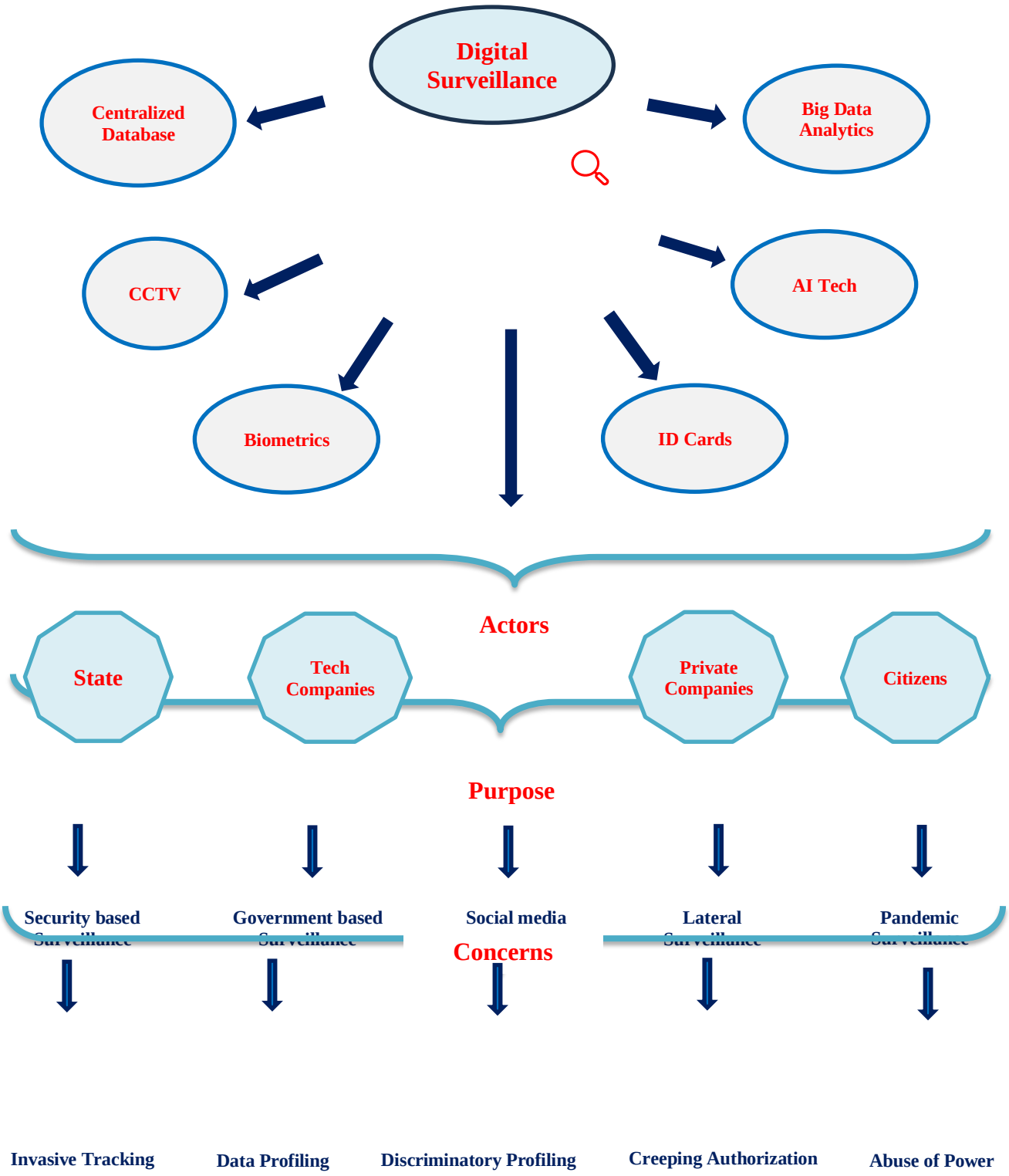
[71] The Digital Personal Data Protection Act, 2023, s 7(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State. *Supra* note 65.

[72] The Digital Personal Data Protection Act, 2023, s 2(l), Data Protection Officer- means an individual appointed by the significant Data Fiduciary under clause (a) of sub-section (2) of section 10*; Supra* note 65.

Thus, the Digital Personal Data Protection Act 2023 is comprehensive legislation that aims to strike a balance between digital surveillance and data privacy. It recognizes the importance of surveillance measures for security purposes while also safeguarding the fundamental right to privacy. The provisions create a framework for organizations and government agencies to protect personal data while still allowing for necessary surveillance measures.

IMPACT OF DIGITAL SURVEILLANCE ON THE RIGHT TO PRIVACY

With the advancement of technology, digital surveillance has become a prevalent issue in society. The use of surveillance technology by government agencies, corporations, and individuals has raised significant concerns about the violation of privacy rights and the possibility of misuse. The ability to monitor individuals' online activities, track their location, and collect personal data without consent raises concerns about the invasion of privacy and the potential for misuse of this information. The challenges posed by digital surveillance to privacy rights are:



1) The diminishing of personal privacy is evident with the widespread use of digital devices and online platforms, where individuals undergo continuous surveillance, and their personal information is gathered without explicit knowledge or consent. This intrusion into private lives gives rise to substantial ethical and legal issues concerning safeguarding personal data and the right to privacy.

2) Another challenge is the lack of transparency and accountability in digital surveillance practices. Many surveillance programs operate in secrecy, without adequate oversight or public scrutiny. This lack of

transparency raises concerns about potential abuse and misuse of surveillance powers. Without proper checks and balances, there is a risk of overreach and the violation of privacy rights.

3) The rapid advancement of surveillance technology presents a challenge in terms of legal and ethical frameworks. With the introduction of new and complex surveillance technologies, lawmakers struggle to keep pace with the development and use of these tools.

4) The digital surveillance raises concerns about the potential for discrimination and profiling. Using algorithms and data analytics in surveillance can target specific groups based on race, religion, or political beliefs. This raises significant ethical concerns and has the potential to intensify existing social inequalities.

5) Another notable challenge presented by digital surveillance is the risk of power abuse by the state and other entities engaged in surveillance. The deployment of digital surveillance tools by law enforcement agencies and government authorities has prompted worries regarding the potential misapplication of these powers.

The impact of digital surveillance on the right to privacy is the loss of autonomy and control over our personal information. With the increasing prevalence of surveillance cameras, social media monitoring, and data collection, individuals are constantly being watched and their activities tracked. The pervasive presence of digital surveillance compromises the right to privacy, which encompasses the ability to control our personal information and make autonomous decisions. Furthermore, Digital surveillance extends beyond national borders, with governments and organizations often sharing information across jurisdictions. This raises concerns about the potential erosion of privacy on a global scale to protect individuals' rights.

CONCLUSION

In conclusion, the implications of digital surveillance on civil rights and privacy represent a complex matter that necessitates thorough examination and assessment. While digital surveillance can serve as a beneficial instrument for law enforcement and national security, it concurrently carries the risk of encroaching upon the privacy and civil liberties of individuals. As technology continues to advance, the potential for surveillance to encroach on individual rights and privacy also increases. It is essential to confront these challenges by establishing a legal and ethical framework that acknowledges and preserves individuals' right to privacy. Digital surveillance should be scrutinized to guarantee its alignment with individuals' protected privacy rights. Although there are valid justifications for employing surveillance in certain scenarios, explicit and precise guidelines must be in place to forestall misuse and guarantee accountability.

Furthermore, it is crucial to acknowledge that digital surveillance also plays a crucial role in maintaining public safety and national security. Therefore, finding a balance between the justified requirement for surveillance and safeguarding privacy and civil rights is essential. Establishing strong legal frameworks and oversight mechanisms is imperative to guarantee that digital surveillance is carried out in a manner that

upholds civil rights and respects privacy. Additionally, the public needs increased awareness and education about digital surveillance's potential risks and implications on their privacy.

****