# BALANCING PRIVACY AND SECURITY: CONSTITUTIONAL IMPLICATIONS IN THE ERA OF CYBER CRIME

Ankit Kumar Yadav, Gujarat National Law University (S)

**ABSTRACT**

In contemporary India, the interplay between privacy and security poses significant challenges under the framework of the Indian Constitution. As cybercrime becomes more sophisticated, the necessity to safeguard national security and public safety must be weighed against the fundamental "right to privacy" as provided by the Constitution. This abstract explores how Indian constitutional principles address this balance, focusing on the right to privacy as recognized in landmark judgments and its implications for cyber security.

The Indian Constitution, particularly through the Supreme Court's landmark Puttaswamy judgement also known as the Aadhar case, has affirmed the right to privacy as a fundamental right under Article 21. This right encompasses protection against arbitrary intrusion and the safeguarding of personal data. The increasing prevalence of cyber threats necessitates robust security measures, such as data collection and surveillance, which can potentially conflict with these privacy rights.

The article examines how Indian cyber security laws, including the IT Act, 2000, and the DPDP Act, 2023 align with constitutional mandates. It delves into the legal and ethical challenges of implementing security measures while ensuring they do not infringe upon individual freedoms. Additionally, it assesses how judicial interpretations, and legislative developments strive to reconcile effective cyber security with respect for privacy.

As we analyse these dynamics, this article shall try to provide a comprehensive understanding of how India navigates the constitutional implications of balancing privacy and security in the digital age, emphasizing the need for policies that protect both personal rights and national interests.

**Keywords:** Privacy Rights, Cyber Crime, Cyber Security Laws, Information Technology Act.

## INTRODUCTION

In recent times rapidly evolving digital landscape, the interaction of privacy and security has emerged as one of the most critical legal and ethical issues. Cybercrime, ranging from financial fraud to cyberterrorism, poses significant threats to national security, economic stability, and public safety. These growing threats necessitate robust cybersecurity measures, including surveillance and data collection. However, such measures often challenge the fundamental right to privacy, as recognized in the Article 21 of the Constitution, as reaffirmed by the landmark Puttaswamy case.[1]

The legal effect which has been attached to a right to privacy is that privacy is needed for a person's liberty, his or her personal integrity, and freedom. Privacy may, however, be restricted for well-recognized state interests such as public protection, security and fighting of crime. The Constitution provides the framework for balancing these competing interests, and courts have played a pivotal role in defining this delicate balance. As cybercrime becomes more sophisticated and pervasive, legal frameworks, such as the IT Act, 2000[2] and the DPDP Act, 2023[3] aim to protect citizens while also safeguarding national security.

India's legal and constitutional structure faces the daunting challenge of ensuring that security measures aimed at combatting cyber threats do not infringe upon the rights as provided by the Constitution.[4] Complexity arises from the need to protect national interests and individual freedoms simultaneously. The concept of "proportionality," as articulated by the Indian judiciary, serves as a guiding principle to navigate this conflict.[5] Under this principle, any state action restricting privacy must be necessary, reasonable, and proportionate to the threat being addressed, ensuring minimal intrusion.

The rise of cybercrime has transformed the way states handle both security and privacy concerns. With increasing threats posed by digital crimes, such as hacking, phishing, identity theft, and cyberterrorism, states often resort to surveillance measures, such as monitoring

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[2] Information Technology Act, No. 21 of 2000, India Code (2000).
[3] Digital Personal Data Protection Act, No. 22 of 2023.
[4] Ritu Gautam, *Proliferation of Cyber Crime and Indian Legal System with Special Reference to Gwalior Division*, https://shodhganga.inflibnet.ac.in/handle/10603/250817 (last visited September 22, 2024).
[5] Amit Singh, Piyush Kulshrestha & Richa Gautam, *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges* (Libertatem Media Pvt. Ltd. 2022).

online activities, gathering data, and regulating digital platforms.[6] However, without stringent legal frameworks, these actions risk violating personal liberties and privacy. The Puttaswamy case underlines this tension, emphasizing that privacy is an inherent right and that any breach must be justified under the strictest standards.

This paper aims to explore these legal dynamics by examining how India balances privacy with security in the context of cybercrime. The analysis will focus on constitutional principles, legislative measures, and judicial interpretations, all of which are critical to understanding the evolving legal landscape in the digital age.

## CONSTITUTIONAL BASIS OF PRIVACY IN INDIA

Right to privacy as provided by Article 21, provides for the right to life and personal liberty.[7] But, the recognition of privacy as a fundamental right was not always explicitly articulated in the early constitutional discourse. The evolution of privacy as a fundamental right can be traced through several landmark cases, with the Supreme Court playing a pivotal role in defining its scope and limitations.

The concept of privacy first emerged in the Kharak Singh's case,[8] where it was a petition that challenged the police surveillance through night domiciliary visits, citing it to be against Article 21. Although the Supreme Court rejected the plea to explicitly recognize privacy as a fundamental right, it acknowledged aspects of privacy by striking down domiciliary visits as a violation of "personal liberty." The Court held that unauthorized intrusion into a person's home constitutes a breach of liberty, thus laying the groundwork for future privacy claims.

Similarly, in the Gobind's case, [9] the Supreme Court acknowledged the right to privacy as an implied right under Article 21, albeit subject to reasonable restrictions. The Court in this case emphasized that privacy is integral to personal liberty, but it can be curtailed if the state demonstrates a compelling interest. This marked the beginning of judicial recognition of privacy, though still limited in its scope.

[6] Anita Singh, Pradeep Kulshrestha & Ritu Gautam, *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges* 149 (Libertatem Media Pvt. Ltd. 2022).
[7] Supra note 1.
[8] Kharak Singh v. State of Uttar Pradesh and Others, (1964) 1 SCR 334.
[9] Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.

## The Landmark Puttaswamy Judgment

The Supreme Court had finally, recognized the right to privacy as a fundamental right in the landmark Puttaswamy case.[10] This case, often referred to as the Aadhaar case, arose from challenges to the government's Aadhaar scheme, which involved large-scale collection of biometric and demographic data. The unanimous ruling of the nine-judge bench stated that the "right to privacy" is a fundamental component of Article 21's, and it also encompasses the Article 14 "right to equality" and Article 19 i.e. "freedom of speech and expression".

In Puttaswamy, the Court laid out key principles for limiting the state's power to infringe upon privacy, notably the "test of proportionality." Under this test, any restriction on privacy must be:

**Legitimate:** A valid state interest, such public safety or national security, must be served by a restriction.

**Necessary:** The state action must be necessary to achieve the intended goal.

**Proportionate:** The measure must not be excessive or disproportionate to the threat it seeks to counter.

This judgment set a new benchmark for privacy jurisprudence in India, directly affecting policies on surveillance, data security and government access to private data.

Following Puttaswamy, several other cases have further clarified the contours of privacy rights in India. In Naz foundation case, which decriminalized homosexuality by interpretation down Section 377 of the Indian Penal Code, the Supreme Court emphasized the intimate connection between privacy and individual autonomy.[11] The judgment held that privacy includes the right to make personal decisions about one's body and sexual orientation, extending privacy beyond physical and informational dimensions to encompass decisional autonomy.

Another significant case where the Supreme Court struck down an RBI circular that restricted financial institutions from dealing with cryptocurrency exchanges.[12] The Court observed that while the government has a legitimate interest in regulating cryptocurrency, such regulations

[10] Supra note 1.
[11] Navtej Singh Johar v. Union of India (2018) 10 SCC 1.
[12] Internet and Mobile Association of India v. Reserve Bank of India AIR 2021 SUPREME COURT 2720, AIRONLINE 2020 SC 298.

must pass the test of proportionality and respect the privacy of individuals engaging in lawful financial transactions.

One of the most significant applications of the Puttaswamy principles came in the Aadhaar judgment.[13] The SC upheld the constitutionality of the Aadhaar scheme but imposed significant restrictions to protect privacy. The Court ruled that Aadhaar cannot be made mandatory for private services such as banking and telecommunications, thus limiting the state's ability to demand personal data without adequate safeguards. The judgment was crucial in balancing the need for a national identification system with the constitutional right to privacy.[14]

### The Role of Article 19 and Freedom of Expression

While privacy is directly linked to Article 21, it is also connected to the freedoms guaranteed under Article 19. The right to privacy extends to freedom given for speech & expression, ensuring that particular persons have the liberty to express themselves without the fear of undue surveillance or data collection. This was confirmed in the 2015 in case of Shreya Singhal, in which the Information Technology Act's Section 66A was declared unconstitutional by the SC for contravening on the right to free speech and expression. This section criminalized inflammatory statements posted online.[15]

In this case, the Court held that surveillance and restrictions on online speech must meet the standards of reasonableness and proportionality. The decision reinforced the view that privacy and free speech are interdependent, and state interference in one domain could threaten liberties in another.

## CYBERSECURITY AND LEGISLATIVE FRAMEWORK

The ever-evolving nature of digital threats, India's legislative & regulatory framework for cybersecurity has undergone significant developments. The primary objective of this framework is to protect individuals, organizations, and the state from cybercrime, while ensuring that security measures Avoid infringement on constitutional rights, particularly the right to privacy. Indian legislation seeks to achieve a compromise between protecting individual liberties and giving the government the authority to stop cyberattacks. This section

[13] Supra note 1.
[14] Ritu Gautam, *Proliferation of Cyber Crime and Indian Legal System with Special Reference to Gwalior Division*, https://shodhganga.inflibnet.ac.in/handle/10603/250817 (last visited September 22, 2024).
[15] Shreya Singhal v. Union of India AIR 2015 SC 1523.

explores the legislative tools that govern cybersecurity in India and their constitutional implications.

**The Information Technology Act, 2000**

India's regulations regarding cybersecurity are still centered around the IT Act. The Act was passed in reaction to the growing use of digital technologies, and it gives authorities the legal framework to deal with cybercrimes such identity theft, hacking, and data breaches.

The IT Act was amended in 2008 to address the growing complexity of cyber threats. The amendments introduced key provisions to handle cybersecurity[16], including:

**Section 43A:** This clause requires businesses that handle sensitive personal data to put reasonable security measures in place. In case of failure, they are liable to pay compensation to affected individuals.

**Section 66:** Addresses offenses related to hacking, with penalties for dishonestly or fraudulently accessing a computer system.

**Section 69**: It empowers the government to monitor, intercept, and decrypt any information for the sake of maintaining public order, national security, or stopping crimes. This provision, while necessary for combating cybercrime, has raised concerns about potential privacy violations.

**Section 66F:** Addresses cyberterrorism and punishes activities that use digital means to jeopardize India's security and integrity.

The IT Act has been instrumental in defining cybercrimes and providing a legal basis for prosecuting offenders. However, as privacy concerns have gained prominence post the Puttaswamy judgment, many have called for amendments to better align with privacy protections.

**Relevant Cases:**

Referring to the 2013 Poona Auto Ancillaries Pvt. Ltd., Pune vs. Punjab National Bank, HO New Delhi & Others[17] case, which resulted in one of the highest awards of compensation in a cybercrime dispute settlement. Rajesh Agarwal, the IT secretary for Maharashtra, had ordered

[16] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
[17] Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank, (cyber) Appeal No. 4 of 2013, Misc. Application No. 120 of 2018.

Bank to give Rs. 45 lakhs to Matharu, the MD of the Pune-based company Poona Auto Ancillaries, who was the grievance. After Matharu received a phishing email, the accused withdrew Rs. 80 lakhs approximately from Matharu's account from the Bank, Pune. According to the claim, the bank did not take the necessary precautions to countercheck bogus accounts formed with the intention of defrauding the person who complained, and the appellant was requested to participate to the loss since he acknowledge to the phishing email.

In the case of Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004[18] Section 67 of the IT Act led to the arrest of Bajaj, the CEO of online website name Bazee.com, for dissemination of cyber pornography. Another individual had offered to sell duplicate copies of digital recording containing sexual data through their services on the website. Regarding Mr. Bajaj, Court observed that he was completely uninvolved in the dissemination of any pornographic content. Additionally, visitors were not allowed to access the sexual content on the Bazee.com website. On the other hand, Bazee.com and other websites rely on advertisements and commissions from sales to generate revenue.

The Court further noted that the information at hand suggests that an individual other than Bazee.com is responsible for the commission of cyberpornography offenses. When the matter was brought before the court, Bajaj was granted release on bond, but only on the stipulation that two sureties, each worth Rs 1 lakh, be produced. It is unpersuasive, nevertheless, because the accused must prove he is only a service provider and does not produce content.

In the case of State of Tamil Nadu v. Dr. L Prakash,[19] FIR was filed in the name of Dr. Prakash under the section 67 IT Act along with the Indecent Representation of Women Act, the Arms Act, and the IPC. The aforesaid matter came into picture when Dr. L Prakash was caught red handed in creating pornographic videos and forwarding the same to US & France to get displayed on X-rated sites. After hearing the defense attorneys' arguments, the fast-track Courts found the accused guilty based on the previously mentioned provisions and sentenced him to life in prison. In addition, he was penalized Rs. 1.27 lakh for breaking the Compensational Afforestation Regulation of 2002. Because sites that are X-rated and its middlemen were detained in India for the first time, this case holds significant precedent for the Cyber Crime Law.

[18] Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2024 (2005)3COMPLJ364(DEL), 116(2005) DLT427, 2005(79) DRJ576.
[19] State of Tamil Nadu v. Dr. L. Prakash, W.P.M.P. No. 10120 of 2002 (Madras H.C. Mar. 15, 2002).

The Suhas Katti case is a precedent in the Cyber Law regime as for the accused that the police and courts have made it possible to have a conviction within mere 7 months of filing of FIR.[20]

The defendant knew the victim on a personal level, and desired to wed her, but she had engaged with another man and got a parted way. That is why, defendant came to her when she was a divorce and when he was unable to have sexual contact with her, he began threatening to marry her online. By exploiting the victim's fictitious email address, the defendant was able to create posts with offensive, derogatory, and annoyance-inducing content about the victim. The accused person was charged under section 67 of the IT Act, 469 & 509 IPC.

Despite the fact that the victim had previously been married and divorced, the defendant continued to have feelings of desire to marry her. The defendant approached her during her divorce, and upon realizing he couldn't have sex with her, he started threatening to wed her on the internet. Using a fictitious email address that belonged to the victim in the account, the defendant posted messages that contained offensive, demeaning, and bothersome information about the victim. The offender was charged in accordance with Sections 469 & 509 IPC and Section 67 of the IT Act. The Additional Chief Metropolitan Magistrate in Egmore claims that there were other violations of the acts. The perpetrator was further sentenced to two years of harsh jail and one year of simple imprisonment under IPC Section 469, in addition to a fine of Rs. 500. RI is subject to a two-year term and a punishment of Rs. 500 under section 509 of the IPC and Rs. 4000 under section 67 of the IT Act.

**Digital Personal Data Protection Act, 2023**

Initiated in 2019, updated in 2022, and set to go into law in 2023, the DPDP Act aims to provide a comprehensive legislative framework for the protection of personal data in India. The Puttaswamy ruling, which emphasized the necessity for strong data protection regulations to preserve privacy, had a significant impact on this measure.

Key provisions of the Digital Personal Data Protection Act[21] include:

> **Data Localization:** The bill requires that sensitive personal information be handled and kept in India. This provision seeks to enhance national security by ensuring that sensitive information about Indian citizens is not accessible to foreign entities.

[20] CC No. 4680 of 2004.
[21] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

**Data Minimization:** It presents the idea of data minimization, which calls on organizations to gather just the minimal amount of information required for a given goal.

**User Consent:** The bill emphasizes the need for informed consent before processing personal data, ensuring that users retain control over their information.

**Exemptions for National Security:** In the sake of maintaining public order, national security, or crime prevention, the bill permits the government to exclude any agency from its rules. While this is necessary for protecting against cyber threats, it has raised concerns about state overreach and the potential for abuse.

The Data Protection Act is seen as a major step in bringing India's cybersecurity laws into compliance with global privacy norms, akin to the General Data Protection Regulation (GDPR) of the European Union.[22] However, its national security exemptions remain contentious, especially in the context of privacy.

**Privacy and Surveillance:** Legal Provisions for Interception and Monitoring

The IT Act's Section 69, along with related rules, grants the government sweeping powers to monitor and intercept digital communications. While these powers are necessary for maintaining cybersecurity and preventing cybercrimes, they raise serious privacy concerns. The SC, in the landmark "Puttaswamy" judgment, made it clear that any irrelevant surveillance must meet the test of proportionality and be subject to strict safeguards.

Along with the IT Act, the Indian Telegraph Act of 1885 permits communication interception for public safety purposes or in times of urgency. The tension between surveillance for security purposes and privacy rights was addressed in PUCL case[23], where the SC established guidelines for lawful interception, emphasizing the need for judicial oversight to prevent misuse.[24]

**The National Cyber Security Policy, 2013**

India's National Cyber Security Policy (NCSP), 2013 was a landmark initiative aimed at strengthening the country's defenses against cyber threats.[25] The NCSP aims to address vulnerabilities in India's critical information infrastructure, such as banking,

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council.
[23] PUCL v. Union of India (1997) 1 SCC 301.
[24] Privacy and Surveillance: Legal Provisions for Interception and Monitoring, in Cyber Law Book, Sharda University, http://cyber-law-book-sharda-u (last visited Sept. 30, 2024).
[25] National Cyber Security Policy, 2013.

telecommunications, and energy sectors. However, despite its intentions, the policy has faced criticism for lacking clear enforcement mechanisms and failing to evolve in response to rapidly changing cyber threats.[26]

The policy focuses on building a secure and resilient cyberspace through:

**Capacity Building:** Encouraging the development of skilled manpower in cybersecurity.
**Public-Private Partnerships:** Promoting collaboration between government, private sector, and academia to improve cybersecurity measures.
**Incident Response:** Establishing a national-level Computer Emergency Response Team (CERT-In) to coordinate responses to cybersecurity incidents.

### Judicial Review of Cybersecurity Measures

Reviewing cybersecurity measures to make sure they don't violate basic rights has been greatly aided by Indian courts. For example, the SC considered whether J&K's internet shutdowns were lawful in case of Bhasin case.[27] The Court determined that prolonged internet shutdowns violate the freedom to freely express oneself under Article 19 and must pass the proportionality test, even though it acknowledged the state's necessity to maintain security.

Similar to this, the SC invalidated Section 66A of the IT Act— which outlawed the use of harsh language online —in the Singhal's case[28] because it was overbroad and ambiguous, infringing on the right provided by Article 19(1)(a). This ruling emphasized how crucial it is to safeguard cybersecurity and digital liberties simultaneously.

### International Cooperation and Cybersecurity

India has also engaged in international efforts to combat cybercrime. It participates in initiatives such as the Budapest Convention on Cybercrime, which seeks to standardize legal frameworks across borders to improve cooperation in fighting cybercrime. While India has not formally ratified the convention, it aligns its cybersecurity measures with global standards,

[26] Nat'l Cyber Sec. Pol'y, 2013, Ministry of Commc'ns & Info. Tech., (2013), available at https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013(1).pdf (last visited Sept. 22, 2024).
[27] Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[28] Shreya Singhal v. Union of India (2015) 5 SCC 1.

particularly in areas like cyber forensics, data sharing, and incident response.[29]

**Ethical Dilemmas: Surveillance and Consent**

The ethical challenges surrounding privacy and security are just as significant as the legal ones. In a world where personal data is increasingly treated as a commodity, the boundaries of ethical surveillance become blurred. Mass surveillance programs, such as India's Central Monitoring System (CMS), aim to protect the country from cyber threats but raise concerns about unchecked state power.[30] The question of informed consent is one of the main ethical issues. People frequently don't know how much information on them is being collected, what is being done with it, or who can access it. For instance, even though the Aadhaar system was created to expedite public services, many individuals were not completely aware of the dangers associated with collecting biometric data and the ways in which third parties may utilize it.[31] This creates an ethical dilemma: Can the state justify infringing on individual autonomy in the name of security without ensuring transparency and consent?

Also, the principle of proportionality has emerged as a key legal and ethical standard to navigate the conflict between privacy and security. This principle, emphasized in the Puttaswamy judgment, requires that any infringement on privacy must be proportionate to the threat it seeks to address. This means the state must demonstrate that its actions are not excessive and that less intrusive means cannot achieve the same result. For instance, discussions over the proportionality of the government's use of Section 69A of the IT Act, which permits it to restrict general usage of internet information, have been triggered. While it can be used to block content that threatens national security or public order, there is a risk that such powers could be misused to suppress dissent or restrict free speech. The challenge is ensuring that these measures are applied with precision and care, maintaining public trust while securing the nation.

To stop cybercrimes, terrorism, and other dangers, mass monitoring systems like the Central Monitoring System (CMS) and NATGRID[32] in India have been established. However, these programs also pose a significant risk to civil liberties if not properly regulated. The potential

[29] Budapest Convention on Cybercrime, opened for signature Nov. 23, 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Sept. 24, 2024).
[30] Central Monitoring System (CMS), Ministry of Home Affairs, Government of India, https://www.mha.gov.in (last visited Sept. 24, 2024).
[31] Aadhaar Act, 2016, No. 18 of 2016.
[32] NATGRID, Ministry of Home Affairs, Government of India.

for abuse of power in surveillance is a serious concern, as it can lead to the breach of personal privacy, unwarranted monitoring of individuals, and even political profiling. In 2015, the SC of India ruled in Singhal that Section 66A of the IT Act, which allowed the government to arrest individuals for "offensive" online posts, was unlawful. The Court found that law breach freedom under Article 19(1)(a) and was vague, leading to potential abuse. This case highlighted how broad surveillance powers, if unchecked, can infringe on not only privacy but also freedom of speech.

## CONCLUSION

The evolving tension between privacy and security in the digital age presents one of the most complex legal and ethical challenges faced by contemporary India. As cybercrime grows in sophistication, the state's need to protect its citizens from these threats becomes more urgent. However, the means by which security is ensured—through surveillance, data collection, and monitoring—must be carefully balanced against the constitutionally protected right to privacy.

The Constitution, particularly through lens of judicial interpretations such as Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017), provides a robust framework to navigate these competing interests.[33] The recognition of privacy as a fundamental right has transformed the legal landscape, ensuring that individual autonomy, dignity, and personal data are protected from arbitrary state action. However, as the Puttaswamy ruling and related judgments have shown, reasonable limitations are allowed and privacy is not inalienable, particularly where public safety or national security is at risk. The legal and ethical challenges lie in ensuring that security measures, such as surveillance and data collection, are proportional to the threat they seek to address and that there are adequate safeguards against potential abuse. "One important tool for achieving this balance is the proportionality test, which was developed by the Supreme Court and stipulates that any invasion of privacy must be justifiable, necessary, and the least invasive course of action".[34] India's legislative framework, particularly the "*IT Act 2000'*,[35] and the '*DPDP Act 2023'*,[36] aims to safeguard personal data while providing the state with necessary tools to combat cyber threats. However, these laws must evolve alongside technological advancements and increasing concerns over privacy. The need for greater

[33] Supra note 1.
[34] Supra note 5.
[35] Supra note 16.
[36] Supra note 21.

transparency, judicial oversight, and strict regulatory mechanisms is crucial to ensure that security measures do not become instruments of mass surveillance or state overreach.

While the balance between privacy and security is delicate, it is not impossible to achieve. Through continued judicial vigilance, legislative reforms, and ethical policymaking, India can develop a legal ecosystem that protects individual rights without compromising national security. Moving forward, a collaborative effort between the government, judiciary, and civil society will be essential to ensure that both privacy and security are upheld in equal measure in the digital age.

## BIBLIOGRAPHY


### Books:

M.P. Jain, *Indian Constitutional Law*, 8th ed. Lexis Nexis, 2018.

Rakesh Kumar Singh & Souvik Dhar, *Media Law Including RTI* (reprint ed., Vinod Publication (P) Ltd. 2024).

J.N. Pandey, *Constitutional Law of India* 57th ed. (Central Law Agency 2020)

Andrew Murray, *Information Technology Law: The Law and Society*, 3rd ed. Oxford University Press, 2016.

Apar Gupta, *Commentary on Information Technology Act*, Lexis Nexis, 2016.Rishika Taneja & Sidhant Kumar, *Privacy Law: Principles, Injunctions, and Compensation*, Eastern Book Company, 2021.

### Reference:

Panday Jyoti, India's Supreme Court Upholds Right to Privacy as a Fundamental Right— and It's About Time, Electronic Frontier Foundation, August 24, 2017, https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

Report of the Group of Experts on Privacy, Government of India, October 16, 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf .

Standing Committee on Access to Information, Privacy and Ethics.Privacy and Social Media in the Age of Big Data, Pierre-Luc Dusseault M.P. Chair, House of Commons Canada,https://www.ourcommons.ca/Content/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf.

Ritu Gautam, Proliferation of Cyber Crime and Indian Legal System, https://shodhganga.inflibnet.ac.in/handle/10603/250817

Privacy and Surveillance: Legal Provisions for Interception and Monitoring, in Cyber Law Book, Sharda University, http://cyber-law-book-sharda-u.

### Websites:

http://www.jstor.org

https://www.researchgate.net/

https://www.coe.int/en/web/freedom-expression/internet

https://heinonline.org