



ARTICLE

Plodded Privacy Law and Nebulous Surveillance

Raju Kumar*, Harshita Shukla**

Abstract

This paper explores the complex and evolving relationship between the right to privacy and the expanding mechanisms of state and non-state surveillance in India. It begins by establishing privacy as an essential facet of human dignity, autonomy, and liberty, while acknowledging that its scope has remained conceptually fluid. Despite the Constituent Assembly's refusal to incorporate explicit protections against unreasonable search and seizure, Indian courts gradually developed privacy jurisprudence, moving from early reluctance in *M.P. Sharma* and *Kharak Singh* to the transformative recognition of privacy as a fundamental right in *K.S. Puttaswamy* (2017). The paper examines how surveillance has been justified in India through legislative frameworks such as the Telegraph Act, Information Technology Act, and Digital Personal Data Protection Act, which grant wide powers with minimal oversight. Through case law analysis, it highlights judicial attempts to balance privacy with legitimate state interests like security, crime control, and public order. It further evaluates emerging forms of surveillance—public, media, and digital—driven by technologies such as AI, data profiling, CCTVs, and spyware, which increasingly blur boundaries between state and private monitoring. The paper concludes that surveillance is inevitable but must be restrained by legality, proportionality, and procedural safeguards to prevent excessive intrusion into constitutionally protected privacy.

Keywords- Right to Privacy, State Surveillance, Digital Surveillance, Constitutional Jurisprudence, Proportionality Framework

I. INTRODUCTION

“*Privacy*” is incessant incident of the human life to keep oneself barricaded from the observance of the others and the society, to entertain uninterrupted reclusion of thought and pursuit, and to steer the control over his preference to engage or withdraw from others, as and when he deems fit, in terms of communication, entitlements, inviolability and information. The term “*Privacy*” has many facets, and it can have many meanings. “*Privacy*” should be treated as one of the most sacrosanct “*fundamental rights*” which should be availed by everyone, subject to “*Reasonable restrictions*.” In “*privacy*”, the person’s pure interest always lies, evident enough from the fact that no reasonable person would entertain the breach of his “*privacy*” at any cost. An individual’s instrumental interest lies with it, which is based on “*fear*”⁴⁵³. It is always a threat that his personal data may be misused against him, even if the leak of the data serves no practical consequences, the encroachment upon his “*privacy*” dreads him. In fact, in some cultures including our own,

* Raju Kumar is an Advocate and LL.M. Candidate at National Law School of India University, Bangalore. He previously served as a Legal Consultant with the Excise Department, Government of Bihar, and currently writes as a Columnist for The Indian Express and The Daily Guardian.

** Advocate, Allahabad High Court

⁴⁵³ Richard A. Posner, *Privacy, Surveillance, and Law*, The University of Chicago Law Review, Winter, 2008, Vol. 75, No. 1 (Winter, 2008), pp. 245-260

such practices can be easily seen where we suffer from “Nudity taboo”⁴⁵⁴. People are generally embarrassed to be seen naked by anyone, particularly when it is with opposite sex. Invasion of “privacy” in such scenario will not hamper him in practical sense but will definitely shatter the mental peace.

As a flip side to the coin of “privacy”, “surveillance” becomes inevitable to the discourse. There is always a legitimate instrumental concealment. It is a fact that publicity hampers communication. “Civil libertarians” want the government to be transparent, but individuals prefer to be opaque; national security is another issue. “Hawks” want the opposite⁴⁵⁵. People hide from the government, and the government hides from the people, and each have their own good or inadequate reasons for concealing from the other. Complete transparency stifles planning and action, while complete opacity jeopardizes both “liberty” and “security”. Terrorists are the most aware of this. Eavesdropping costs innocent people because their “privacy” is violated, but it costs terrorists far more because it completely disrupts their plans and puts them in danger of capture or death and this illustrates how “surveillance” can work both as an angel and a demon. Interpretation of the term “surveillance” has varied time to time and case to case which demonstrates a dire lack of understanding of the width of this term. Various facets of “state surveillance” in India are interception of communication via telegraph, CCTVs, “Peer to peer techniques” with advancement of informational technology such as “Arogya Setu” App tracking individuals with infection during Corona Pandemic, etc., which brought Indian cities like Delhi, Mumbai and Chennai on top ranks in Forbes list of the most surveilled cities in the world.⁴⁵⁶

II. PRIVACY AND CONSTITUTIONAL ASSEMBLY DEBATE

The Indian constitution, influenced by common law and the Fourth Amendment, aimed to codify the “right to privacy”, a concept that was not yet established in the “European Convention on Human Rights”⁴⁵⁷ or “Universal Declaration of Human Rights”⁴⁵⁸. The Constituent Assembly failed to seriously consider the “right to privacy” in drafting the “Fundamental Rights”, leading to an amendment against “unreasonable searches”.

The Indian Constitution’s “Fundamental Rights” Chapter, proposed by Kazi Syed Karimuddin, aims to protect against “unreasonable search and arbitrary seizure”⁴⁵⁹. Two proposed “privacy” insertions to the Indian Constitution, one addressing “unreasonable search safeguards”⁴⁶⁰ and the other “protecting correspondence privacy”⁴⁶¹, were rejected with minimal debate. Dr. Ambedkar accepted Karimuddin's proposal, but the majority vote was contentious. The Vice-

⁴⁵⁴ *Id.* at. 1.

⁴⁵⁵ Arindrajit Basu, Extraterritorial algorithmic surveillance and the incapacitation of international human rights law, 12 NUJS L. Rev. 2 (2019).

⁴⁵⁶ Forbes India, <https://www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1>, (last visited Oct. 25, 2025).

⁴⁵⁷ European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_ENG, (last visited Oct. 26, 2025).

⁴⁵⁸ United Nations, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>, (last visited Oct. 26, 2025).

⁴⁵⁹ Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly of India (3-12-1948).

⁴⁶⁰ Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly of India (3-12-1948).

⁴⁶¹ Constituent Assembly Debates, Volume VII, Part II, Constituent Assembly of India (6-12-1948).

President attempted to put the Karimuddin text to vote twice but Mr. T.T. Krishnamachari objected, claiming the majority vote was against the amendment. Unrest in the house led to Jawaharlal Nehru's proposal to postpone the vote, which proved controversial. Eventually, Karimuddin's amendment was defeated with no debate, resulting in the privacy principles safeguarding citizens from intrusive search and seizure being never inserted into the Constitution⁴⁶². The Constituent Assembly made its decision with little meaningful debate on the subject.

III. RIGHT TO PRIVACY – INTERNATIONAL SCENARIO

The “right to privacy” or “Privacy” has been a topic of discussion around the globe. However, in most occasions the term has been remained unclear and vague. Let us have a look on the jurisprudential aspect of this in other jurisdictions.

United States

Initially, the US Constitution didn't provide the “*Right to Privacy*” explicitly. However, later in 1791 “*Fourth Amendment*” was introduced to protect the American people from unreasonable searches and seizures.⁴⁶³ The Supreme Court on several occasions have interpreted various amendments to state that such right exists. It was in the Year 1974, when the “*Privacy Act*”⁴⁶⁴ was passed with the intention to protect their citizens from third party infringement.

Germany

It is one of the countries, which enforces the “*Privacy*” laws in a strict sense. In fact, the traces of “*privacy*” can be found in Article 2 of the “*Constitution of Germany*”⁴⁶⁵. Indeed, in the recent past, Germany's “*Privacy*” law has caused significant difficulty to big firms such as Facebook and Google, who operate on the foundation of internet freedom.⁴⁶⁶

Canada

Privacy law in Canada has developed over time since it was first enacted in 1977 as part of the “*Canadian Human Rights Act*”⁴⁶⁷. Initially, the law was enacted to protect personal data. The law was amended in the year 1983 to place a restriction on how the government can obtain and share personal information. The last time the law on privacy changed was in the year 2012, when the Court of Appeal, Ontario recognized that the Common Law in Canada accepted the right to personal private as a “*tort of intrusion upon seclusion*”⁴⁶⁸.

⁴⁶²Chinmayi Arun, Paper-thin safeguards and mass surveillance in India, 26 NLSI Rev. 105-114 (2014).

⁴⁶³Ronald Reagan Presidential library and Museum, <https://www.reaganlibrary.gov/constitutional-amendments-amendment-4-right-privacy>, (last visited Oct. 26, 2025).

⁴⁶⁴Office of Privacy and Civil Liberties, <https://www.justice.gov/opcl/privacy-act-1974>, (last visited Oct. 26, 2025).

⁴⁶⁵Federal Ministry of the Interior and Community, <https://www.bmi.bund.de/EN/topics/constitution/constitutional-issues/constitutional-issues.html#:~:text=The%20current%20version%20of%20the,the%20Federal%20Republic%20of%20Germany.&text=The%20Basic%20Law%20was%20adopted,the%20state%20until%20German%20reunification>, (last visited Oct. 26, 2025).

⁴⁶⁶Kerber, W., Zolna, K.K. The German Facebook case: the law and economics of the relationship between competition and data protection law. Eur J Law Econ 54, 217–250 (2022), <https://doi.org/10.1007/s10657-022-09727-8>.

⁴⁶⁷Government of Canada, <https://laws-lois.justice.gc.ca/eng/acts/h-6/>, (last visited Oct. 26, 2025).

⁴⁶⁸Jones v. Tsige, 2012 ONCA 32 (CanLII)

Sweden

Alongside being one of the first countries in the world to provide its residents with a “*Personal identification number*” that must be used in all interactions with the state, Sweden is also one of the first countries to establish a detailed statute on “*online privacy rules*”. The “*Data Act of 1973*”⁴⁶⁹ safeguarded the privacy of personal data stored on computers. The Swedish constitution under its Chapter 8, Article 7⁴⁷⁰ has also Protected the “*right to personal data protection*”.

European Union.

The “*European Union's Data Protection Directive*”, enacted in 1995, governs the handling of personal data within the EU. Article 8 of the “*European Convention on Human Rights (ECHR)*” guarantees the right to privacy and family life, subject to certain limitations.⁴⁷¹

IV. INDIAN LEGISLATIONS ON PRIVACY AND SURVEILLANCE

From the legislative lens, apart from the procedural laws of the country which provide for the police surveillance there are a few legislations namely- “*Information Technology Act*,”⁴⁷² and the “*Indian Telegraph Act*,”⁴⁷³ along with “*Digital and Personal Data Protection Act*,”⁴⁷⁴, “*Indian Wireless Telegraphy Act*,”⁴⁷⁵ and “*Telegraph Cables (Unlawful Possession) Act*,”⁴⁷⁶ that accommodate the new- age surveillance techniques. S. 69 of the IT Act⁴⁷⁷, empowers the government to direct any agency or government to “*monitor*”, “*decrypt*” or “*intercept*” any information in or from a computer resource. However, no legislative supervision mechanism has yet been devised over these powers. “*Central Monitoring System*” (hereinafter referred as CMS) is a big name in India’s surveillance regime which, through algorithms, enables the government to monitor all our online activities and intercept telephonic and electronic communications.⁴⁷⁸ CMS has massive dossiers of our “*Sensitive Personal data*” which is unfetteredly accessible to the government and secret agencies in the name of national security, along with “*National Intelligence Grid*” (NAT-GRID), “*Lawful Intercept And Monitoring Project*” (LIM), “*Crime and Criminal Tracking Network & Systems*” (CCTNS), and “*Networking Traffic Analysis*” NETRA, which picks up on trigger words such as “*terror*”, “*kill*”, “*attack*”, etc. And *Nira Radia*⁴⁷⁹ case brought in light that it’s not always that government follows the procedures while dealing with the data of citizens. Even under “*Digital Personal Data Protection Act*,”⁴⁸⁰ the government has been exceptionally given the unrestricted right to retain the data of the citizens which could be

⁴⁶⁹Information Policy Country Report: Sweden, [https://deepblue.lib.umich.edu/bitstream/handle/2027.42/64844/IPOL%20country%20report%20-%20Sweden%20\(2009\).pdf;sequence=1](https://deepblue.lib.umich.edu/bitstream/handle/2027.42/64844/IPOL%20country%20report%20-%20Sweden%20(2009).pdf;sequence=1), (last visited Oct. 26, 2025).

⁴⁷⁰ *Id.* at 17.

⁴⁷¹ European Convention on Human Rights, *supra* note 5.

⁴⁷² The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁴⁷³ The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).

⁴⁷⁴ The Digital Personal Data Protection Act, 2025, No. 22, Acts of Parliament, 2025 (India).

⁴⁷⁵ The Indian Wireless Telegraphy Act, 1933, No. 17, Acts of Parliament, 1933 (India).

⁴⁷⁶ The Telegraph Wires (Unlawful Possession) Act, No. 74, Acts of Parliament, 1950 (India).

⁴⁷⁷ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁴⁷⁸ Addison Litton, The State of Surveillance in India: The Central Monitoring System’s Chilling Effect on Self-Expression, 14 WUGS L. Rev. 800 (2015).

⁴⁷⁹ *Ratan N. Tata v. Union of India*, MANU/SC/1056/2013

⁴⁸⁰ The Digital Personal Data Protection Act, 2025, No. 22, Acts of Parliament, 2025 (India).

deftly used to create a 360° profile of an individual in the name of national security and is purported to be used for future references defying the “purpose limitation”⁴⁸¹- basis of data protection laws.

FOUNDATION OF RIGHT TO PRIVACY IN INDIAN COURT: AN ANALYSIS

These legislative exemptions trammel the judiciary from examining the government on questions of “privacy” with respect to data surveillance. While in a lot of cases only the “police surveillance” was under scrutiny but in yet other cases the court narrowly interpreted the compass of the term surveillance falling into constant conundrums between “right to privacy” vis- a- vis “surveillance”. The term “Privacy” has not been used anywhere in the constitution. However, the court in different judgments have evolved this concept. The first such instance was of “M.P. Sharma v. Satish Chandra”⁴⁸² where “Surveillance” was given more importance as being state’s overriding power due to the reason that the Constituent Assembly did not think it fit to adopt the American “fourth Amendment” in the Indian settings. But this judgment did not address the “right to privacy” on the whole rather only in respect of the “Search and Seizure” i.e., “police surveillance”. Approx. 9 years later in the case of “Kharak Singh v. State of Uttar Pradesh”⁴⁸³ keeping a watch over someone of the character of history sheeter in the interest of the state was not held to be the infringement of “privacy” because it’s not a guaranteed right under the constitution. These judgments contemplate “privacy” as proprietary concept yet were unreceptive to recognizing the “right to privacy”. Though concurring but Subba Rao J. said that “privacy” is essential extension of “right to liberty” and thus, all surveillance measures in his opinion are unconstitutional.

A Balanced approach was adopted in “*RM Malkani v State of Maharashtra*”⁴⁸⁴, a case about the constitutionality of phone tapping. Up until now the courts refused to recognize any *privacy* right within the contours of art. 21⁴⁸⁵ and had justified the violations on the grounds of “*targeted persons*” i.e., history sheeters or guilty persons. In “*Gobind v State of MP*”⁴⁸⁶, the court recognized the “*right to privacy*” but also brooded upon its restriction, which following the American jurisprudence shall be for “*compelling public interest*”⁴⁸⁷, a restrictive ground stringent in nature than those qualifying Art. 19⁴⁸⁸ rights, however was limited by the “*narrowest tailoring concept*” which corresponds with the “*proportionality*” test of India. The good side however is that in this case the supreme Court recognized “*privacy*” as an aspect of “*liberty*”. In “*Malak Singh v. State of P&H*”⁴⁸⁹ the SC has followed the same lines as previous cases i.e., restricting “*surveillance*” to the serious criminals and repeat offenders but has also provided for judicial review upon the “*surveillance*” by providing that the SP has to satisfy the court of the

⁴⁸¹ Reversing Privacy Risks, <https://ctlj.colorado.edu/wp-content/uploads/2025/09/LL-Final-08.02.2025.pdf>, (last visited Oct. 26, 2025).

⁴⁸² M.P. Sharma v. Satish Chandra, MANU/SC/0047/1954

⁴⁸³ Kharak Singh v. State of Uttar Pradesh, MANU/SC/0085/1962

⁴⁸⁴ RM Malkani v State of Maharashtra, MANU/SC/0204/1972

⁴⁸⁵ INDIA CONST. art. 21.

⁴⁸⁶ Gobind v State of MP, MANU/SC/0119/1975

⁴⁸⁷ Locke v. Davey 540 U.S. 712 (2004).

⁴⁸⁸ INDIA CONST. art. 19.

⁴⁸⁹ Malak Singh v. State of P&H, MANU/SC/0157/1980

beliefs that satisfied him to run surveillance against a person. But the question before such an interpretation and fancy adoptions of American concepts is- how would it explain the constant state action of profiling individuals not having any criminal record or tendency to become a threat to the society at large? Following the same lineage of thought the court rejected “*bulk surveillance*” as it prescribed for the surveillance of specifically declared people and places only based on reasonable suspicion and belief that the information could not be acquired by any other less breaching method limited to the purposes of s. 5(2) of the “Punjab Police Act”.

“*In Manohar Lal v. UOI*”⁴⁹⁰, Supreme Court took a way forward “*The judiciary cannot avoid discussing national security out of fear that it may be brought up as a defense.*”

In “*PUCL v. UOI*”⁴⁹¹, telephone tapping was held to be the infringement of the “*right to privacy*” one has, to hold conversations in the “*privacy*” of one’s home or office, termed as “*technological eavesdropping*”. In “*State of Maharashtra v. Bharat Shanti Lal Shah*”⁴⁹² court permitted the communication can be intercepted under the “*Procedure established by law*”. This might seem a regressive approach from the lens of freedom but seems more convincing because any facet of life can’t be left unregulated, to certain extent state must have power to breach the “*privacy*” specially for the cause of national security and criminal justice system. The Apex court outrightly exclaimed in “*PUCL v. UOI*”⁴⁹³, “*privacy*” is not an absolute right and is subservient to the security of state. In “*Collector v. Canara Bank*”⁴⁹⁴ the court came back to the question of “*privacy*”- with respect to the issue of search and seizure and said that “*Touchstone of reasonable and proportionality*” is a must when it comes to legislative enactments or executive or judicial orders which curtail the “*right to privacy*”. Same jurisprudence was followed in the cases of “*P. R. Mitrani v. CIT*”⁴⁹⁵, “*Ram Jethamalani v. UOI*”⁴⁹⁶ and “*Ratan N Tata v. UOI*”⁴⁹⁷ all of which were relating to police surveillance. Additionally, in these cases the court adopted the person specific approach of “*privacy*”, thus, even in a public place, some “*surveillance*” activities could amount to infringement of privacy.

A new form of police surveillance was explored by the judiciary in “*Selvi v. State of Karnataka*”⁴⁹⁸ where the court considered the conducting of “*BEAP test*” and “*polygraph test*” as infringement of “*Mental privacy*”.

In 2017⁴⁹⁹, deciding the legal validity of the Aadhar database considering the “*right to privacy*”, a nine-judge bench over-ruled the “*MP Sharma*”⁵⁰⁰ and “*Kharak Singh*”⁵⁰¹ judgments holding that “*right to privacy*” is an integral part of “*right to life and personal liberty*” as well as that of “*dignity, autonomy and liberty*”. The court for the first time measured the extent of the right and said, “*It was not a narrow right against physical invasion, or a derivative right under Article 21, but one that covered the body and mind, including decisions, choices, information*

⁴⁹⁰ Manohar Lal v. UOI, C/Cr Jurisdiction, 2021 INSC 100 .

⁴⁹¹ PUCL v. UOI, MANU/SC/0149/1997

⁴⁹² State of Maharashtra v. Bharat Shanti Lal Shah, MANU/SC/3789/2008

⁴⁹³ PUCL v. UOI, MANU/SC/0188/2004

⁴⁹⁴ Collector v. Canara Bank, MANU/SC/0935/2004

⁴⁹⁵ P. R. Mitrani v. CIT, MANU/SC/0362/2006

⁴⁹⁶ Ram Jethamalani v. UOI, MANU/SC/0711/2011

⁴⁹⁷ Ratan N. Tata v. Union of India, MANU/SC/1056/2013

⁴⁹⁸ Selvi v. State of Karnataka, MANU/SC/0325/2010

⁴⁹⁹ Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., MANU/SC/1044/2017

⁵⁰⁰ M.P. Sharma v. Satish Chandra, MANU/SC/0047/1954

⁵⁰¹ Kharak Singh v. State of Uttar Pradesh, MANU/SC/0085/1962

and freedom.”⁵⁰² Non adoption of the Fourth amendment doesn’t imply the negation of the “right to privacy” in India. Court additionally held that “right to privacy” is not an absolute right and state can exercise “surveillance” over it upon the fulfilment of the requirements of legality, need in terms of the “legitimate state aim” and “proportionality” of the measures adopted, to which Justice S.K. Kaul added a fourth one- “procedural guarantees against abuse of such interference”. However, it prescribed certain parameters of judicial review “in cases of intrusion by the State in the “privacy” of an individual” i.e., compelling state interest is to be searched for, only in case calling for “strict scrutiny” while in other cases standard of reasonability under Art 21 would suffice.

In the light of the fact that Fundamental rights can be enforced against “non- state actors” as well if they perform public duties or functions or statutory activities that impact the right of citizens.⁵⁰³ as well as the judicial activism in “*Bodhisattwa Gautam vs. Subhra Chakraborty*”⁵⁰⁴, where interim compensation was awarded holding that fundamental rights under Article 21⁵⁰⁵ are enforceable even against private bodies and individuals, it becomes inescapable from the observation that “Surveillance” is effectuated by not just the government but also non state actors.

V. SURVEILLANCE — EMERGING TRENDS

A. Surveillance by public

“*Surup Singh Nayak v. State of Maharashtra*”,⁵⁰⁶ a case against an RTI demanding the details of hospitalization of a convict, court held that in favor of larger public interest the medical records could be disclosed and thus the “right to privacy” of the person could be legitimately breached. Disclosure of information about the assets and liabilities of the electoral candidates⁵⁰⁷ and judges⁵⁰⁸ owing to the “Public Interest test” under Section 8(1)(j) of the RTI Act has been held justified. That is why the Apex court in “*R Sukanya v R Sridhar*”⁵⁰⁹ did not permit the publication of the proceedings relating to matrimonial matters and justified the S.22 of the “Hindu Marriage Act, 1955”⁵¹⁰ providing for in camera proceedings because it involved no public interest.

B. Surveillance on personal choices

“Right to privacy” includes “right to make personal choices”. “Surveillance” entails keeping watch over a person or his activities or information. It is hence limiting on the individual’s autonomy, impacting how that individual interacts with the world.⁵¹¹ “*Freedom of Religion Acts*” enacted by various states prescribes for the pre- requisite of declaration of the intention to convert to another religion to the District magistrate. This implies the record- keeping and watch- over upon the essentially personal decision making of an individual which ideally must be

⁵⁰² Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., MANU/SC/1044/2017

⁵⁰³ Kaushal Kishore v. State of UP WP Cr. No. 113 OF 2016.

⁵⁰⁴ Bodhisattwa Gautam vs. Subhra Chakraborty, MANU/SC/0245/1996

⁵⁰⁵ INDIA CONST. art. 21.

⁵⁰⁶ Surup Singh Nayak v. State of Maharashtra, MANU/MH/0170/2007

⁵⁰⁷ PUCL v. UOI, MANU/SC/0235/2003

⁵⁰⁸ CPIO Supreme Court of India v. Subhash Chandra Aggarwal, MANU/DE/2714/2009 .

⁵⁰⁹ R Sukanya v R Sridhar, MANU/TN/9201/2004

⁵¹⁰ Hindu Marriage Act, 1955, No 25, Act of Parliament, 1955 (India).

⁵¹¹ IEP, <https://iep.utm.edu/surv-eth/> (last visited Sept. 24, 2025).

autonomous. The court in *Navtej Singh Johar v. UOI*⁵¹² has explicitly said that “Autonomy is individualistic” and has recognized self- expression of LGBTQ community freeing them from the criminality under S. 377 IPC⁵¹³ which was a diminution on their autonomy to choose their sexual orientation and indulge in sexual activity with whomsoever they desire.

C. Media Surveillance

Unbridled gathering of information and following around individuals is an unconcealed modus operandi of the media. It enfolds sting operation which was held repugnant to law by the apex court in “*BMW hit- and – run*”⁵¹⁴ case and laid down whole set of guidelines in this respect in the “*Uma Khurana*”⁵¹⁵ case; and squatting at the houses and places the celebrities and other people of eminence traverse, which stretches to the insensitive coverage as was the case with Sushant Singh Rajput’ death which was challenged in “*Nilesh Navlakha v. UOI*”⁵¹⁶ and was checked by the court on the basis of the public policy doctrine.

D. Digital Surveillance

In present era, apart from physical inviolability, which is the traditional connotation of “*privacy*”, information has become the most vulnerable dimension out of all the end number of aspects of “*privacy*”, thanks to the technological revolution that has hastened vast dissemination of information and encouraged mass indulgence. These impeccable capabilities of contemporary media and information system has kept the “*privacy*” at peril. In present info- technological era, mutual interaction between the internet and the masses has opened up gates for intermediaries to collect sensitive data of all, so they have capability of profiling every individual and infringe our “*privacy*”. So, we consider the question of “*privacy*” not just with respect to the state, but also the private entities which satisfy the qualifications handed down by the Kaushal Kishore⁵¹⁷ judgment. Digital Intermediaries use automated tools like AI, algorithm and techniques as far as neurotechnology to collect and analyze the data and profile individuals making them far more surveilling than state. Current surveys show that the government leeches off of the “*surveillance*” by the private entities for monitoring and muzzling the expression of dissenting citizens. Instances of arrest for posting allegedly objectionable content on the social media sites, for instance, two boys from UP arrested for posting objectionable cartoons of “Prime Minister Modi” and “Chief Minister Yogi Adityanath”, is quite prevalent these days. This retrogresses the exercise of autonomy by citizens in political engagement and political expressionism. Another monstrous instance of “*digital surveillance*” was the “*Pegasus spyware*” which was alleged to have entered in the devices of multiple eminent personalities of India from diverse fields. Following “*DRC v. Canara Bank*”⁵¹⁸, “*right to privacy*” is about person not places, so even in a public place a person can’t be said to have lost his “*privacy right*”. This warrants the mentioning of the unique tracking technique via CCTVs acquired by the State of UP against people causing damage to the state property during riots and mobs which involves their identification based on the CCTV image and tracking of their address, domiciliary visits, arrests and penalization. Such

⁵¹² *Navtej Singh Johar v. UOI*, 2018 INSC 790 .

⁵¹³ Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

⁵¹⁴ *R K Anand v. Registrar*, Delhi High Court, MANU/SC/0291/2009

⁵¹⁵ *Court On Its Own Motion v. State*, MANU/DE/1662/2007 .

⁵¹⁶ *Nilesh Navlakha v. UOI*, MANU/MH/0044/2021 .

⁵¹⁷ Surup *supra* note 54.

⁵¹⁸ *Ratan supra* note 45.

profiling and tracking via technology though efficient and essentially for the state purposes is nonetheless a form of “surveillance”.

VI. CONCLUSION

No right is ever absolute and so is the right to privacy as also affirmed by the apex court in the "*K S Puttaswamy*"⁵¹⁹ judgment. Unrestricted interpretation of the right would enable people to justify anything and everything. There seems to be an inherent need to legitimize some sort of checks and balances on the exercise of the right, given that courts have now adopted the “person-specific approach” with regard to “*privacy*”. Limitations on a right don't seem to be beneficial to “*liberty*”, yet occasionally, especially in contemporary contexts, it becomes necessary to monitor and check on private behavior. This is achieved through “*surveillance*”. In the context of the traditional connotation of Surveillance i.e., “*police Surveillance*”, it goes without saying how the absence of such mechanism would hamper the efficacy of the criminal justice system and therefore, “*privacy*” can be invaded for investigation, public purpose and “*national security*”. In the current era, however, we witness many different forms of “*surveillance*” such as “*public surveillance*”, “*media surveillance*”, “*digital surveillance*”, etc.

Without these limitations, citizens would be able to justify violating social norms including “*morality*”, “*decency*”, “*integrity*”, “*dignity*”, and “*culture*” in the name of “*privacy*”. Consider wearing indecent clothing in public in the name of exercising the “*right to make any personal choice*”, which is a facet of the “*right to privacy*”, or expressing communally or nationally offensive or defamatory opinions online, which one could argue is justified in the name of “*privacy*” even if it has the effect of inciting communal violence and interfering with social settings, or a ton more similar instances where individualistic approach to the enjoyment of rights sway people to disregard the national and social order and norms. In this regard, we have seen how “*public surveillance*” checks flaunting of decency and morality and “*digital surveillance*” is a cure to “*political disinhibition*”.

It makes it quite clear that the need for “*surveillance*” is unavoidable. However, “*surveillance*” must be subject to its own limitations because it runs the risk of being incompatible with the “*right to privacy*” and going too far infringing on that right. In the “*Puttaswami*”⁵²⁰ decision, the supreme court purposefully made allowances for “*surveillance*” upon the fulfilment of the requirements of “*legality*”, “*legitimate state aim*” and “*proportionality*” of the measures adopted.

⁵¹⁹ Justice *supra* note 50.

⁵²⁰ Justice *supra* note 50.