Educational Administration: Theory and Practice
2024, 30(1), 1189-1198
ISSN: 2148-2403
https://kuey.net/

Research Article

Data Privacy And State Surveillance: An Analysis Of Competing Interests In The Indian Context

Dr. Lohit Sardar[1*]

[1*]Assistant Professor, BRM Govt. Law College, Guwahati, Email ID:lohitsardar6@gmail.com

Citation: Dr. Lohit Sardar (2024) Data Privacy And State Surveillance: An Analysis Of Competing Interests In The Indian Context, *Educational Administration: Theory and Practice, 30(1),* 1189-1198
Doi: 10.53555/kuey.v30i1.6073

ARTICLE INFO

ABSTRACT

The burgeoning digital landscape of the country presents a complex interplay between an individual's right to data privacy in the digital arena and the State's need to engage in surveillance activities in the interests of security and public order. The dichotomous relationship sits at the crux of the debate presented within this present paper, and the paper attempts to understand and analyze the intricate relationship of these competing interests. The paper delineates the laws governing surveillance practices in the state, and subsequently, explores and examines the development of the laws of privacy, that coincidentally have evolved when questions regarding the extent of permissible surveillance in the nation have been raised, and in this context, seeks to carve out a legal framework wherein surveillance is permitted only within the aegis of the existing jurisprudence of privacy rights. Through a critical analysis of the existing jurisprudence from both sides of the debate, the paper also looks towards the American and European legal positions governing the dichotomous position of data privacy vis-à-vis surveillance, and seeks to understand the position that has been adopted therein, with an aim to inculcate some of the principles evolved there into the Indian legal framework.

Keywords – Right to Privacy, Data Privacy, Digital Surveillance, Surveillance State, Personal liberty and dignity.

1. INTRODUCTION

The burgeoning expansion of digital information in the 21st century has led to the generation of millions of gigabytes of digital information on a daily basis. This has raised concerns about allied rights, with the primary issue being that of digital privacy. Although neither the notion of privacy in the traditional sense, which has existed for at least a century in legal jurisprudence; nor the notion of digital privacy, whose presence can be found in the annals of European law since the 1980s onwards, are new concepts in the outright sense, its implementation in Indian law is still at a very nascent stage. This is because although the right to privacy has been recognized in various capacities over the years by the Indian judiciary, despite not being an explicitly prescribed right within the constitutional fold, it has only recently been deemed to be a fundamental right within the aegis of Article 21 in the landmark case of *"Retd. Justice Puttaswamy v. UOI"*[1](hereafter *Puttaswamy* judgement) judgement.

This recognition has opened a Pandora's Box of rights, including the right to data privacy, yet, these developments have also led to the development of certain legal conundrums that need to be addressed and balanced. One of the foremost challenges being posed against privacy rights in the digital arena stems from the issue of national security, wherein the interests posed by the societal concerns of national security take a diametrically opposed legal position to the individual interests encapsulated within data privacy rights. The recent *sub-judice* matter in the Delhi HC, between the Government of India (hereafter GOI) and WhatsApp regarding the constitutionality of Section 4(2) of the *"Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021"*that allows the decryption of private digital information forcertain reasons, which, *inter alia,* also include *"purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State",*is a primary example of the dichotomous position that these conflicting interests occupy.

[1] (2017) 10 SCC 1 503.

It is against this backdrop that the present paper will attempt to understand and analyse the implications of data privacy rights within Indian law vis-à-vis issues of state surveillance in the interests of national security, with an aim to balance these contradictory interests. The first chapter is an introduction to the paper. The second chapter will look at the laws governing surveillance in India. The third chapter will delve into the development of the right to privacy, which ultimately evolved into the right to data privacy, and how the competing interests of surveillance and privacy rights have been dealt with in Indian jurisprudence. The fourth chapter will provide a brief overview of the foreign legal position by analysing European and American jurisprudence. The fifth chapter will undertake an analysis to critically examine how the competing rights of data privacy and surveillance can be balanced in the Indian context. Finally, the sixth chapter will summarise the arguments in the paper and conclude the discussion.

2. SURVEILLANCE LAWS IN INDIA: AN OVERVIEW

Privacy is not an unlimited right since bestowing the privilege of being unlimited in its scope to any legal right is not in the interests of justice. The status of data privacy within law also occupies a similar position since it itself is a facet of individual privacy. This implies that the right to privacy must also yield to certain interests that are more sacrosanct in their nature and scope. The interests of the State, especially with regard to tenets of State security, is undoubtedly one of the considerations for which privacy, and data privacy as well, must bow. The interests of the nation as a whole will unsurprisingly trump individual interests, yet, the legal conundrum that arises herein lies in determining the limits that allow such infringement on privacy in the wider and larger interests of the State.

In Indian law, a number of legislations govern surveillance laws. The *"Telegraph Act, 1885"* allows the State to*"intercept calls"* if the same is done in the –*"interests of the sovereignty and integrity of India; security of the state; friendly relations with foreign states or public order; preventing incitement to the commission of an offence."* Furthermore, there are two basic preconditions that are necessary for applying this section – *"occurrence of any public emergency"* and *"in the interest of public safety"*. Interestingly, these are the same restrictions that have been mentioned under Article 19(2) as legitimate restrictions on the freedom of right to free speech and expression within the aegis of Article 19(1). Notably, though, this provision extends only to physical records and does not extend directly to digital information, and therefore, does not directly violate the tenets of data privacy.

Subsequently, the *"Information Technology Act, 2000"* (hereafter IT Act, 2000) was passed, and under Section 69, it allows the State to *"intercept, monitor and decrypt"* information that has been either generated or transmitted digitally through a computer resource, in the interests of *"sovereignty & integrity of India; friendly relations with foreign States; defence of India; maintenance of public order; or, prevention of any cognizable offence."* Furthermore, the *"Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009"* governs the procedural notions that bestow the right upon 10 surveillance agencies to *"intercept, monitor and decrypt"* information within any computer resource. The three words – intercept, monitor or decrypt are considerably wider in their ambit than the powers bestowed within the Telegraph Act, 1885, and considering that they are not limited by considerations such as the physical presence of the data source which necessitates physical proximity to the same, the surveillance powers are exponentially enhanced since any digital information or data can be monitored or decrypted within the territorial confines of the nation without the knowledge of the data subject to whom the data belongs. It also negates encryption mechanisms, which are otherwise efficient enough in safeguarding individual data from prying eyes, and grants the State blanket impunity to surveil individuals in the digital realm. Additionally, the two grounds –*"the interests of public safety"* and *"occurrence of any public emergency"* are missing from the IT Act, 2000 and therefore, these two threshold tests are absent when surveillance is done by following the provisions of the IT Act, 2000.[2]

Finally, the *"Digital Personal Data Protection Act, 2023"* (hereafter DPDP Act, 2023) which was recently enacted to deal with data privacy and protection in India needs to be discussed. Inherently, the legislation was designed to function for preserving the rights of the individuals vis-à-vis their privacy rights in the digital realm, especially after the *Puutaswamy Judgement*. For example, it mandates under Section 4 that processing individual data is only permitted if it has been consented to by the data principal, and if the same is being done for a lawful and legitimate purpose. Yet, the legislation legitimises surveillance and widens the ambit of the State in exercising surveillance powers within the digital realm.This is because Section 7(c) of the DPDP Act, 2023 allows the State and its instrumentalities to engage in non-consensual data processing of private individuals if done *"in the interest of sovereignty, integrity and security of state, maintenance of public order or preventing incitement to any cognizable offence"* yet, it fails to enumerate and define the ambiguity surrounding the enabling phrases. In other words, the legislation does not clarify the extent of the terms "integrity and security of the state" and "maintenance of public order", and considering the wide amplitude of these terms, as well as the variegated domains that fall within their ambit, it gives blanket protection to the State in processing personal data of individuals with impunity. Similarly, in Section 17(c), it

[2] Chaitanya Ramachandran, *"PUCL v. Union of India Revisited: Why India's Surveillance Law Must be Redesigned for the Digital Age"*, 7 NUJS Law Review 111 (2014).

is provided that the provisions of Chapter II, which primarily deals with the rights of individuals regarding data privacy, except two sub-sections of Section 8, shall be inapplicable if the*"data is being processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India."*This is another blanket provision that precludes the application of data protection norms, and since it exists in domain of criminal behavior, it allows the State to engage in curtailment of the guarantees prescribed in the DPDP Act, 2023 by citing the probability of the commission of any criminal act, thus allowing the violation of data privacy rights of the individual.

Thus, two primary criticisms arise in the Indian context vis-à-vis laws governing surveillance. Firstly, the laws themselves are widely worded, thereby bestowing upon the State the widest possible powers of construction and interpretation to justify and maintain the legality of their acts of surveillance. Secondly, the discretionary power to implement surveillance on individuals is solely vested upon the executive and is not limited by any oversight from any institution, be it the Parliament or the legislature,[3] with the only remedy being the judiciary if an individual knocks on their doors. Against this backdrop, it is pertinent to understand the development of privacy rights, which have developed primarily due to judicial activism in India, with an aim to understand how the courts have dealt with the debate of surveillance v. privacy.

3. PRIVACY AND DATA PRIVACY: AN ANALYSIS OF INDIAN JURISPRUDENCE

The genesis of data privacy can be traced from the wider rights of privacy. Data privacy is therefore merely a facet of privacy rights, brought forth by the expansion of technology, and merely expropriates privacy to the digital realm. Therefore, the notion of data privacy is in its nascent stages, especially within Indian jurisprudence, and therefore, any discussion on the notion of data privacy needs to also a discussion on privacy in general. In this context, the chapter will first briefly elucidate the development of privacy and data privacy in global jurisprudence before moving on to the development of the same within Indian jurisprudence.

3.1 HISTORY OF DATA PRIVACY IN GLOBAL JURISPRUDENCE: A BRIEF OVERVIEW

Historically, the concept of individual privacy has existed within common law from at least the 16th century, with the *"Semayne Case"*[4] declaring the sanctity of an individual's premises by stating - *"the house of everyone is to him as his castle and fortress."* J. Blackstone has also commented in this regard as – *"so particular and tender a regard to the immunity of a man's house that it stiles it his castle, and will never suffer it to be violated with impunity.*[5]*"* With time, the principle that privacy only protected *"one's castle"* began to erode, and evolution of the principle led to a gradual development wherein other facets of life were also incorporated within the domain of individual privacy. Warren & Brandeis, in their seminal article on this topic in the last decade of the 19th century, discussed privacy as "the right to be self alone" and opined that the development of technology would make the recognition of this right more sacrosanct than ever before. They said - *"……so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury"*[6] and discussed that the *"inviolate personality"* includes within itself the right to *"exclude others from our thoughts, sentiments and emotions."*[7]

Over time, the expansion of privacy norms also included within itself data privacy. The primary bastion of data privacy norms was Europe. The advancements in computing technology mandated that data protection also be considered an important aspect of privacy norms. The *"Organisation of Economic Co-Operation and Development"* (hereafter OECD) had laid down certain guidelines pertaining to the protection of data privacy, and these encompassed 8 broad principles – *"collection limitation; data quality; specification of purpose; limitation of use; reasonable security safeguards; openness; individual participation; and, accountability*."[8]Subsequently, a data protection regime was envisaged within Europe in the form of the European Union Data Protection Directive in 1995, and this functioned as the primary norm governing data protection until the enactment of the more comprehensive *"General Data Protection Regulation, 2016"*[9] (hereafter GDPR, 2016).

---

[3] Vrinda Bhandari & Karan Lahiri, "The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World"3(2) *University of Oxford Human Rights Hub Journal,* 17 (2020).

[4] 77 Eng. Rep. 194 (K.B. 1604).

[5]William Blackstone, *Commentaries on the Laws ofEngland* 168 (Oxford Clarendon Press, 1769).

[6] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" 4(5) *Harvard Law Review* 196 (1890).

[7]*Ibid.*

[8]Sanjay Sharma & Pranav Menon, *Data Privacy and GDPR Handbook* 28 (Wiley, 2020).

[9] Gianmarco Cifaldi, "Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development" 7(1) *Sociology and Social Work Review* 43 (2023).

3.2 THE INTERTWINED HISTORY OF PRIVACY AND SURVEILLANCE IN INDIA: THE JUDICIAL JOURNEY FROM KHARAK SINGH TO PUCL

In India, privacy as a distinct right has been afforded recognition only through judicial interpretation. The Constitution of India does not contain any specific provision that delineates privacy as a specific right. Similarly, there is no legislative recognition granted to the right to privacy. This makes the evolution of privacy rights a necessary study in understanding the development of the notion of data privacy. Interestingly, the initial developments of the law related to privacy have been derived from discussions related to the power of surveillance that the State possesses, and therefore, the nascent beginnings of this right within Indian jurisprudence are traceable to the conflicting concerns of surveillance in the interests of State security vis-à-vis individual privacy.

The first inroad for recognising this right under Indian law was made in *"Kharak Singh v. State of Uttar Pradesh"*[10], wherein the UP Police Regulations bestowed powers of surveillance on *'history sheeters'*, individuals that are notorious for repeated offences albeit not always charged for the same. The Hon'ble SC took note of the necessity of this right, and for the first time in Indian jurisprudence, gave the right to individuals, and also invalidated the nightly domiciliary visits that the impugned regulation permitted. Apart from being the first explicit recognition afforded to the right to privacy in Indian law, it is significant for two jurisprudential developments. Firstly, an argument by the State that the surveillance norms were directed only against individuals that were suspected on proper grounds, and therefore, necessitated certain restraints vis-à-vis their rights due to the anti-social activities that they partook in, was accepted by the Court when it opined that – *"such a classification would have an overwhelming and even decisive weight in establishing that the classification was rational and that the restrictions were reasonable and designed to preserve public order by suitable preventive action."*[11]Secondly, in his dissenting opinion, J. Subba Rao opined that although the Constitution does not give an explicit recognition to the right to privacy, it is nevertheless a sacrosanct part of the right to personal liberty, and he defined privacy as *"the right to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures."*[12] Apart from this, Subba Rao also held the right to privacy to flow from the facet of personal liberty contained within Article 21,[13] and this would subsequently function as the bedrock for the recognition afforded to the right in *Puttaswamy*.

Interestingly, prior to this, when a similar question was posed before the Court in *"M.P Sharma v. Satish Chandra"*[14], the Court had refused to recognise any limitations on the power of the State to engage in search and seizure, and had stated that since the makers of the Constitution had outrightly rejected the recognition of a right analogous to the Fourth Amendment of the American Constitution, which safeguards individuals and their privacy from unreasonable searches, the judiciary cannot impose such a limitation on the State. Therefore, within a decade, the judiciary had overruled its initial position.

A decade later, questions similar to *Kharak Singh* once again emerged in *"Gobind v. State of Madhya Pradesh"*[15], and provisions of the Police Act of 1861 that allowed surveillance to prevent the commission of offences in repeat offenders were challenged, with the primary issue being domiciliary rights vis-à-vis surveillance. The decision reiterated the position of privacy vis-à-vis its earlier position and also elevated the status of the same to the position of a constitutional right. Thus, privacy became a constitutional right, a position which would again be reiterated in *"R. Rajagopal v. State of Tamil Nadu,"*[16] and in *Rajagopal,* the right to privacy was deemed to be implicit within the ambit of 'personal liberty' under Article 21. Interestingly, *Gobind* also states - *"assuming that the right to personal liberty, the right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them. It must be subject to restriction on the basis of compelling public interest. But the law infringing it must satisfy the compelling state interest test."*[17]Therefore, this judgement was significant in pointing out that although privacy is a right that is encompassed within Indian jurisprudence, it nevertheless does not amount to an unlimited right, albeit the limitations that are to be placed on the right must satisfy a compelling interest of the State; yet, in proclaiming the same, it did not elucidate what would amount to *'State interest'* and provided the ambiguity surrounding this phrase, the impunity granted to the State undoubtedly risks unsolicited violations of privacy, especially when weighed against privacy.

The next major development occurred in *"PUCL v. Union of India"*.[18]Herein, the judiciary recognised for the first time the dichotomous position of surveillance laws vis-à-vis the right to privacy that had been given ample recognition under Indian jurisprudence, and when Section 5(2) of the *"Indian Telegraph Act, 1885"*

[10](1964) 1 SCR 332.
[11]*Ibid.*
[12]*Ibid.*
[13]*Ibid.*
[14] AIR 1954 SC 300.
[15]AIR 1975 SC 1378.
[16] 1994 SCC (6) 632.
[17]*Supra Note* 17.
[18] (1997) 1 SCC 301.

was challenged, the Court, while asserting its constitutionality, realized the significance of bestowing procedural protections, and in this pursuit, gave a few guidelines. Firstly, orders for tapping telephones could only be issued by the Home Secretary of a State or Union Government; secondly, the authority must consider the reasonable possibility of acquiring the information sought through other means; thirdly, orders for surveillance under this legislation Will have a temporal duration of two months from their issuance; fourthly, review committees must be constituted to evaluate the legality of the orders; and fifthly, the authority issuing the orders must maintain records of all the intercepted information.[19] These guidelines were subsequently incorporated into Rule 419-A of the *"Indian Telegraph Rules, 1951",* with certain modifications, such as fixing the total period of interception at 180 days[20] and that senior law enforcement officers will have the discretion to issue orders for starting surveillance when directions from the Home Secretary are not possible, with such orders confirmed by the appropriate authority within seven working days.[21] After the passage of the IT Act, 2000, these guidelines also translated to the Rules governing surveillance under this legislation,[22] and therefore, the impact of the guidelines by the Court in the *PUCL judgement* also has ramifications or data privacy in the digital era.

3.3 CANARA, PUTTASWAMY, AADHAAR AND BEYOND: THE MODERN POSITION OF PRIVACY

The *PUCL judgement* was a significant development primarily because the Court had actively attempted to set forth guidelines for delineating the extent to which the State could engage in surveillance, and aimed to safeguard the right to privacy. However, over the next two decades, three judgements furthered the cause of privacy rights vis-à-vis surveillance in India to new heights.

The first of the three is the *"Collector v. Canara Bank"*[23] wherein section 73 of the *"Stamp Act, 1899"* was questioned for allowing infringement of privacy rights by granting a right to the Collector to access private records that were otherwise confidential between the banker and customer. The Court made three important observations in this case – firstly, it opined that privacy was a right designed to protect the 'person' and not the 'place' and as such notwithstanding where the property of a person was, the right would continue to protect the confidentiality of the contents of the property; secondly, surveillance practices must be targeted and in the presence of reasonable suspicion; and, thirdly, it held that if a legislative provision enables the violation and abuse of privacy rights, notwithstanding the remoteness of the possibility of such violation, the legislation's constitutionality can be subjected to doubt and apprehension.[24]

The *Puttaswamy* judgement brought another paradigm shift to the domain of privacy rights in Indian jurisprudence. While the right had developed independently, and with reference to State surveillance, over many decades, its constitutional position was still unclear. Yet, with this judgement, the 9-judge bench of the Apex Court held that the right to privacy emanated from the sacred trio of fundamental rights – Articles 14, 19 and 21, and that *"privacy is the ultimate expression of the sanctity of the individual"*[25] This placed privacy at a very high pedestal in the hierarchy of rights. The Court further delineated a few procedural protections that must be complied with before the right can be infringed –firstly, legality, implying that whatever restriction or limitation is being placed on the right, the same must have a legal validation; and secondly, the test of proportionality, wherein there must be a legitimate nexus between the infringement of privacy being contemplated and the objective that such an infringement seeks to fulfill and that the infringement should be balanced in the sense that it should only be in accordance of the need.[26]

Finally, the judgement in *"Justice K.S. Puttaswamy v. UOI,"*[27](hereafter Aadhaar Judgement) commonly known as the *Puttaswamy II,* needs to be discussed. In this judgement, the foundational principles regarding privacy that were formulated in the *Puttaswamy Case* were put to the test for analysing the constitutionality of the *"Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016"* (hereafter Aadhaar Act, 2016). Two important questions, *inter alia,* were presented before the Court – firstly, is the Aadhaar Act, 2016 enabling the government to function as a surveillance State; and secondly, whether the information collected by the Aadhaar system was an infringement on the privacy that the *Puttaswamy judgement* had guaranteed. Regarding the first question, held that the Aadhaar Act, 2016 did not necessarily lead to the creation of a surveillance State because the structure of the Aadhaar collected only *"minimal biometric data"* that could not be used for surveilling individuals, however, considering the concerns, it directed that authentication records must not be stored by the government for a period longer than six

[19]*Ibid.*
[20]Indian Telegraph Rules, 1951, Rule 419- A(6).
[21]*Ibid,* Rule 419-A(1).
[22] Ramachandran, *Supra Note* 04, at 112.
[23] (2005) 1 SCC 496.
[24] Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" 26(2) *National Law School of India Review* 148 (2014).
[25]*Supra Note* 01.
[26]*Ibid;* see also, Bhandari & Lahiri, *Supra Note* 05, at 24.
[27](2019) 1 SCC 1.

months, a period which was a drastic reduction from the five years permitted under the Act. Regarding the second question, the Court relied upon the requisite protectionary necessities mandated in the *Puttaswamy judgement* - legality and proportionality and highlighted that although the principle of legality was fulfilled, the proportionality test remained unfulfilled since it allowed, under Section 139AA of the IT Act, 2000 for mandatory linkage between the Aadhaar and PAN cards, and thus, the provision of mandatory linkages was struck down for infringing on privacy rights.

4. AMERICAN AND EUROPEAN POSITION: A BRIEF OVERVIEW

4.1 AMERICAN POSITION

The United States of America has had a contentious history with surveillance and privacy, especially State-sponsored intrusion into individual privacy. During the American Revolutionary War, the founding fathers detested the issuance of *"general warrants"* and *"writs of assistance"* that *"allowed the ransacking of personal papers"* and *"sweeping searches without an evidentiary basis"* respectively, and this detestation of the infringement of privacy rights led to the enactment of the three significant amendments of the U.S. Constitution.[28] The Third Amendment protects privacy within the limits of the dwelling premises and states - *"no Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law";* the Fourth Amendment safeguards the rights that people have for securing their *"persons, houses, papers and effects"* against searches that are unreasonable in nature; and, the Fifth Amendment safeguards against self-incrimination.[29] American law therefore has already given adequate safeguard and constitutional protection against governmental surveillance and intervention vis-à-vis privacy, and considering the constitutional position of these rights, it is sensible to conclude that they also extend to and address the requirements brought forth by technological changes, including the extension of the right to safeguarding interests in the digital realm.

Interestingly, the decision taken by the American SC in *"Katz v. United States"*[30] gives an important insight. It states that the Fourth Amendment's protection applies not merely to proprietary items such as homes and dwelling places but to areas wherein there exists a *"reasonable expectation of privacy."*Again, in another case *"United States v. Jones"*[31], it was held that GPS tracking on an individual's phone to track his movements over 28 days was a violation of the rights under the Fourth Amendment, amounting to physical trespass, and the reliance upon long-term digital surveillance would inevitably be a violation of the individual's reasonable expectation of having privacy. This ultimately paved the way for law enforcement agencies to obtain a warrant prior to indulging in electronic surveillance, especially if it was for a long-term tracking, and thus, undoubtedly bolstered privacy rights from being infringed by modern technology through the monitoring of digital data.

4.2 EUROPEAN LAW

Data protection and privacy have historically been very significant considerations under European jurisprudence, and the fact that Europe has historically been the bastion from which data protection and privacy norms have flowed is a testament to the significant role that this continent has played in furthering this right. The primary law dealing with Data Privacy in the European context is the GDPR, 2016 and it states under Article 5 that personal data must be processed in a way that is fair and transparent; that it should be collected only for specific and legitimate purposes without being used for any purpose incompatible with the specified one; and that it should be relevant and limited to the objective. Furthermore, Article 15 of the GDPR, 2018 specifies that the data subjects must be informed by the data controller about the processing that their personal data undergoes, along with the purpose for which it is being processed, and the data subjects are also empowered to object against processing of personal data if it is done for profiling.

The *"Court of Justice of the European Union"*(hereafter CJEU) has recently given some interesting insights. In the first case,[32] the Court was more inclined towards safeguarding privacy rights, and it opined that the *"EU Privacy and Communications Directive 2002/58"* and the *"EU Charter on Fundamental Rights"*(hereafter EUCFR)are significant because they prevent the processing and retention and transmission of personal data, such as traffic and location data, even if the same is being done in the interests of national security. In the second case,[33] the Court took a slightly more balanced stance and stated that if the member states can prove the *"existence of legitimate and serious threats that pose a threat to national security"*, then EU law does not preclude the retention or transmission of data for surveillance purposes, albeit it also noted that in such cases, the data must be retained only for a "strictly necessary period" and stated that the decision

[28] Daniel J. Solove, "A Brief History of Information Privacy Law" in *Proskauer on Privacy A Guide to Privacy and Data Security Law in the Information Age* (Practising Law Institute, 2016).

[29]The Constitution of the United States of America, 1789, 3rd, 4th& 5th Amendments.

[30] 389 U.S. 347 (1967).

[31] 565 U.S. 400 (2012).

[32] Case C–623/17 Privacy International ECLI:EU:C:2020:790.

[33] La Quadrature Du Net and Ors., C-512/18 (2020).

of such data intrusion should be subjected to review by either a court or an independent administrative body. The general consensus from the CJEU has usually reflected a stance that echoes the position taken by it in the *"Privacy International Case,"* since in the *"Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources"*[34]case from2014, it had invalidated the *"Data Retention Directive"* for disproportionately interfering with the right to privacy in individual life[35] and data protection.[36] Therefore, the European position has granted a lot of importance and significance to data privacy and placed it above nonchalant surveillance by the State, thus safeguarding the interests of the common individual from being infringed by the State.

5. DATA PRIVACY AND SURVEILLANCE IN INDIA: SHORTCOMINGS, CHALLENGES AND A SEARCH FOR BALANCE

The protection of privacy rights in the era of digitisation remains a critical challenge primarily because of technological progress in the domain of Information and Communication Technology (hereafter ICT) through digitisation of information, blurring the boundaries between the traditional apparatus used for surveillance and the digital devices that are used in everyday lives, thus making surveillance more intrusive into the private and personal lives of individuals.[37] The introduction of *"big data"* has revolutionized the actions of the Surveillance State. It is no longer limited in its scope and domain to relying on merely traditional forms of surveillance, and instead, it can afford to utilise the digital information generated daily by individuals to further its interests in national security. The State has the capability of utilising a vast array of means for gathering data – "*wiretapping; video-graphing; geolocation tracking; data mining; intercepting, decryption and monitoring of emails; and, tracking internet and social media usage"*[38]and each of these mechanisms is an infringement of the traditional notions of data privacy, causing a furore in the legal standard vis-à-vis the position of individual rights. Interestingly, this was also noted by J. Kaul in his concurring opinion in the *Puttaswamy judgement,* when he noted – *"the growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable."*[39]

Against his backdrop, one of the key challenges that is posed towards law enforcement agencies or state entities engaged in surveillance is the amount of infringement on individual privacy that they must engage. The agencies who are engaged in surveillance harbour the idea that it is necessary to collect vast amounts of data, including gathering personal data and information from individuals to get an understanding of issues that are potentially harmful – terrorism, cyber attacks or other forms of harm for example.[40] The question that arises herein is – to what extent is the curtailment of privacy rights for facilitating and furthering surveillance done in the pursuit of State security justified?

The judicial opinion has largely favoured societal interests over individual rights. For example, it has been observed in *"Mardia Chemicals v. UOI"*[41] that when public interest to a considerably large degree is involved, individual rights may have to bow down and give way if it is necessary to achieve the object wherein public purpose is being served. Again, in the context of privacy vis-a-vis larger public interests, it was opined in *"Rohit Shekhar v. Narayan Dutt"*[42], it was observed by the Delhi HC *"forced interventions with an individual's privacy under human rights law in certain contingencies has been found justifiable when the same is founded on a legal provision; serves a legitimate aim; is proportional; fulfils a pressing social need; and, most importantly, on the basis that there is no alternative, less intrusive, means available to get a comparable result."*Again, in *"Ritesh Sinha v. State of Uttar Pradesh"*[43] it was observed by the Hon'ble SC that the fundamental right to privacy as envisaged in the *Puttaswamy judgement* cannot be construed as absolute and instead it must bow down to larger public interests. National security is one of the foremost considerations that drive the policy decisions of any sovereign government since it is pertinent that these governments remain vigilant and careful against national and international issues that threaten their interests.[44] When weighed against this backdrop, and if one considers surveillance done in the interests of

[34] [2014] All E.R. (EC) 775.
[35] European Union Charter on Fundamental Rights, Art. 07.
[36]*Ibid,* Art. 8.
[37] Johann Čas et.al., (eds.), *Surveillance, Privacy and Security Citizens' Perspectives* 03 (Routledge, 2017).
[38]Bhandari & Lahiri. *Supra Note* 05, at 17.
[39]*Supra Note* 01.
[40] Debasish Nandy, "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns"1 *Journal of Current Social and Political Issues* 14 (2023).
[41] [2004] 4 SCC 311.
[42] (2011) SCC OnLine Del. 4076.
[43]AIR 2019 S 3592.
[44]Moulinath Moitra & Akash Chatterjee, "National Security and Privacy - Which Side Will the Debate Move?" 2(2) *Indian Journal of Integrated Research in Law* 04 (2022).

State security to fall within the bracket of public interest, which it rightly should, given the significance of safety and protection that nations strive to ensure for their citizens, data privacy rights must undoubtedly indulge surveillance laws.

Yet, what if the notion of *'compelling state interest'* that was evolved in *Gobind judgement* is taken? It was highlighted in the discussion of the *Gobind judgement* itself that the Court failed to elucidate what would amount to such an interest, yet, if one looks at the doctrine's roots, it is traceable from American jurisprudence, wherein this goes hand in hand with the doctrine of *'narrow tailoring'* which states that the State is *"burdened to demonstrate that the restriction placed on a right in the context of a compelling State interest is done in such a manner that it infringes the right in the narrowest possible manner to achieve the goals."*[45] If one considers the positions that the DPDP Act, 2023 and the IT Act, 2000 grant the State vis-à-vis examination of private data of individuals, it does not fulfil the doctrinal necessities of the *Gobind* judgement.

Interestingly, the Justice B.N Srikrishna Committee Report, which was a report submitted by a 10-member committee constituted under the chairmanship of Retd. J. B.N. Srikrishna to frame a data protection bill for India, had recommended that the Government incorporate legislative provisions for governing the oversight committed during intelligence gathering activities of the government,[46] yet, as seen from the DPDP Act, 2023, the legislation not only fails to limit surveillance activities vis-a-vis data privacy, it also emboldens the State. If anything, it takes a position that is completely opposed to respecting norms surrounding data privacy and instead grants the State a degree of legislative impunity to the State to infringe on individual rights. The legislation is explicitly silent as far as protectionary principles about surveillance are concerned, and contrarily, it instead validates non-consensual data processing by granting the State a plethora of exemptions. Unfettered powers bestowed upon the State to collect and process data of individuals in the interests of vaguely coined terms such as "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 cognisable offence relating to any of these" are distinctly detrimental to individual rights.

Critics have also opined that the uptake of mass surveillance of digital information by state authorities goes hand-in-hand with the reformulation of the *"classical notion of national security"* with the same being less interested in territorial defence and more concentrated in profiling citizens for the protection of the state.[47] The process of profiling refers to classification of individuals - their tastes, preferences and practices, with an aim to predict future behaviour, and exposes the individual's life to transparency from the State's perspective.[48] The chilling effects of profiling have already been practically witnessed in the *Cambridge Analytica* issue. One way of dealing with this issue would be to provide safeguards in consonance with the provisions of the GDPR, 2018 that prevent profiling of individuals without their consent, and this would also inevitably operate as a significant restriction against unabated surveillance. Another issue that stems from this is the inherent promise associated with the privacy-security trade-off wherein it is argued that increased surveillance will also lead to a proportionate increase in security, yet, this not merely leads to a misallocation of resources for security measures in the short run, but also can be detrimental in identifying the primary issues of insecurity in the long run.[49] These issues ultimately negate the right to data privacy when weighed against surveillance concerns of the State.

A stringent application of the tests developed in *Puttaswamy judgement* and reinforced further through the *Aadhaar judgement* can undoubtedly prove to be a necessary safeguard for the individual vis-à-vis their privacy rights in the digital arena. Uncontrolled surveillance and profiling can be addressed if the tests of legality and proportionality, as well as the necessity of a rational nexus between the infringement of individual privacy and surveillance, are satisfied prior to undertaking surveillance initiatives.

6. CONCLUSION

The world today lies on thecusp of a digital revolution. The internet has brought forth a paradigm shift in the domain of ICT. However, the digitization of information and data has exponentially increased the risk of creating a surveillance State, since the digitization of data has enabled the State to encroach on the digital presence of individuals with greater immunity and impunity. This is primarily due to the non-physical nature of digital data that is not restricted by traditional limitations and also the bestowal of anonymity that snooping in the digital realm grants when compared to physical surveillance. Allegations that a spyware

[45] Grutter v. Bollinger, (2003) 539 US 306; see also, Bhatia, *Supra Note* 26, at 135-36.

[46] Sonali Srivastava, "India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL" *Indian Journal of Law and Technology Blog,* 21 Mar 2024< https://www.ijlt.in/>.

[47]Bigo, D. (2006) "Protection. Security, Territory and Population", in J. Huysmans et.al., (eds.) *The Politics of Protection. Sites of Insecurity and Political Agency* (Routledge, 2006).

[48]Enrico Maestri, "Surveullance and Profiling, Online Person's Privacy Between Criminogenic Structures and Legal Paternalism" 3(2) *Journal of Ethics and Legal Technologies* 61 (2021)

[49] Čas et.al., *Supra Note* 39.

named Pegasus was being used to spy on certain prominent personalities[50] show the potential risks that unabated surveillance can have on individual privacy in India. In another example, in a *sub-judice* matter before the Apex Court, the Indian State has revealed through a document that was not within the public domain that it has been surveilling through electronic means according to a *"Standard Operating Procedure"*,[51] a phrase which reeks of ambiguity and opacity. These examples highlight the grim possibility of the Indian State becoming a*"Surveillance State"* wherein data privacy rights give way to digital surveillance, more often than not done without the consent or knowledge of those being spied upon.

Indian law has been instrumental in recognizing privacy rights, often through judicial intervention, and the law of privacy has developed hand-in-hand with the law of surveillance. The judiciary has tried to balance these interests over the years, yet, with the digitization of information, a plethora of new challenges have arisen that need to be addressed. Data privacy is at the heart of the debate, and although data protection and privacy are being safeguarded to some extent, the degree of protection bestowed may not be enough to ensure that the State itself does not infringe upon these rights under the garb of surveillance done in the interests of the State.

Therefore, it is necessary that some changes be made to the existing scenario. Three suggestions are being made in this regard:

Firstly, the legal framework needs a comprehensive and robust framework that focuses on data protection and privacy vis-a-vis surveillance. An expectation that a constitutional amendment akin to the American position should be introduced into the Indian Constitution as well may be too far-fetched in Indian jurisprudence, however, an amendment within the DPDP Act, 2023 with an aim to place privacy at a higher pedestal than surveillance, and wherein processing of personal data needs to go through a range of safeguards akin to the position of the GDPR, 2018 can be a more realistic expectation. The DPDP Act 2023 failed to live upto the expectations as far as balancing the competing interests of privacy and surveillance are concerned; however, an amendment that addresses the existing shortcomings can be a probable solution.

Secondly, oversight authorities can be formulated. The judiciary can be the primary oversight authority responsible for protecting individuals from excesses in the infringement of their right to privacy and considering the historical context wherein the judiciary has been the primary benefactor of the Indian citizen as far as bestowing privacy rights is concerned, this would be in consonance with the historical activism exhibited by the judiciary. Considering the overburdened position of the judiciary, it may not be possible or feasible for the judicial bodies to deal with such infringements directly, yet, a quasi-judicial body, governed on judicial principles, can be another probable solution for bringing balance.

Finally, there needs to be greater awareness among the general populace regarding their rights in the digital realm, primarily the rights to data protection and privacy. It is because only a more robust and informed citizenry can ensure that their rights are protected, and considering the nuances involved in balancing privacy norms against surveillance done in the interest of the State, the presence of an informed citizenry that can understand the need for a balance in these competing interests is undoubtedly a necessity.

REFERENCES

1. DidierBigo, (2006) "Protection. Security, Territory and Population", in J. Huysmans et.al., (eds.) The Politics of Protection. Sites of Insecurity and Political Agency (Routledge, 2006).
2. Chaitanya Ramachandran, "PUCL v. Union of India Revisited: Why India's Surveillance Law Must be Redesigned for the Digital Age", 7 NUJS Law Review 111 (2014).
3. Daniel J. Solove, "A Brief History of Information Privacy Law" in Proskauer on Privacy A Guide to Privacy and Data Security Law in the Information Age (Practising Law Institute, 2016).
4. Debasish Nandy, "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns" 1 Journal of Current Social and Political Issues 14 (2023).
5. Enrico Maestri, "Surveullance and Profiling, Online Person's Privacy Between Criminogenic Structures and Legal Paternalism" 3(2) Journal of Ethics and Legal Technologies 61 (2021)
6. European Union Charter on Fundamental Rights, 2000.
7. Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" 26(2) National Law School of India Review 148 (2014).
8. Gianmarco Cifaldi, "Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development" 7(1) Sociology and Social Work Review 43 (2023).
9. Indian Telegraph Rules, 1951.
10. Johann Čas et.al., (eds.), Surveillance, Privacy and Security Citizens' Perspectives 03 (Routledge, 2017).
11. Moulinath Moitra & Akash Chatterjee, "National Security and Privacy - Which Side Will the Debate Move?" 2(2) Indian Journal of Integrated Research in Law 04 (2022).
12. Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" 4(5) Harvard Law Review 196 (1890).
13. Sanjay Sharma & Pranav Menon, Data Privacy and GDPR Handbook 28 (Wiley, 2020).

[50]Wasim Raza, "The Impact of the Recent Pegasus Spyware Controversy on the Rights to Privacy in India", 2(2) *Doon Journal of Multidisciplinary Research* 157 (2023).

[51] Bhandari & Lahiri, *Supra Note*05, at 16.

14. Sonali Srivastava, “India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL” Indian Journal of Law and Technology Blog, 21 Mar 2024 < https://www.ijlt.in/>.
15. The Constitution of the United States of America, 1789, 3rd, 4th& 5th Amendments.
16. Vrinda Bhandari & Karan Lahiri, “The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World” 3(2) University of Oxford Human Rights Hub Journal, 17 (2020).
17. Wasim Raza, “The Impact of the Recent Pegasus Spyware Controversy on the Rights to Privacy in India”, 2(2) Doon Journal of Multidisciplinary Research 157 (2023).
18. William Blackstone, Commentaries on the Laws of England 168 (Oxford Clarendon Press, 1769).