KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 01 Issue 01 KnowLaw

History of General Data Protection Regulation and Evolution of Concept of Surveillance in International and Indian Context.

Lovika Jaiswal[1]

Abstract

In the era where technology has become indispensable, the world is moving with the accelerated pace and slight delay in communication can hamper the daily work to a great extent. The internet is rampant and its users are omnipresent. The details divulged by Edward Snowden about NSA's surveillance regime in 2013 led to a lot of legal and policy questions all across the globe. The article analyses the question of how other countries across the globe operate with and entertain surveillance. The article throws light on the history of General Data Protection Regulation of the European Union. It helps to understand the evolution of the concept of Surveillance. The article analyses the evolution of surveillance through law in India as well. It also addresses the question as to what extent the data should be monitored and extracted by the public authorities?

Introduction

The term surveillance is derived from two etymological terms 'sur' which means 'from above', and 'veillance' which means 'to watch'. The term surveillance has gained substance and has got a new meaning since the 1960s. The area under surveillance has been extended exponentially and this spread has triggered multidisciplinary research on surveillance. Starting from Closed-Circuit Television (CCTV) cameras placed in cities and all around the corners of the streets, the surveillance has been extended to digital world i.e. the computers which covers call tapping, data encryption, etc. It indicates that the types and scope of surveillance has increased.

[1] 03rd Year, LL.B., Campus Law Centre, University of Delhi, LovikaJasiwal78@gmail.com

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 01 Issue 01 KnowLaw

Theoretical debates on evolution of Surveillance - Why Surveillance?

Panopticon: Bentham and Foucault.

Panopticon is the architectural figure proposed by Bentham in 18th century after his visit to his brother's factory in Russia. The principle on which the architectural design of the factory was based on is "central inspection". When Bentham returned to his home country, he tried to persuade the then Prime Minister to organize all the architectural structures, not just prisons but also factories, schools and hospitals. A number of prisons have incorporated panopticon; one of the prominent examples is- the Presidio Modelo complex in Cuba, infamous for cruelty, which is now abandoned.

Every panopticon is an architecture with a watch tower at the core of the structure with a watchman in it. There are small rooms around the circumference from where inmates can't see the watchman but watchman can see the inmates. Therefore, as Foucault rightly stated that "visibility is a trap"[2] in a panopticon. The idea of keeping a constant watch on people is a way of exercising power, enormous power. Though the action is discontinuous the effect of surveillance is constant. The effect is constant because the "visibility trap" induces the conscious of inmates and it is resulting in automatic functioning of power. In lieu of this Bentham laid down a principle that "power should be visible and unverifiable"[3]. Visible in the sense that the inmates can constantly see the tower that they are being watched from, and unverifiable in the sense that they still don't have any idea if somebody is really looking at them or not; to make it unverifiable to an extended way it is ensured that even the shadow of watchman is not visible to the inmates.

[2] Brunon-Ernst (Ed.), *Beyond Foucault: New perspectives on Bentham's panopticon* (pp. 1–16). (2013). Surrey: Ashgate Publishing.
[3] Brunon-Ernst, A., & Tusseau, G. Epilogue: the panopticon as a contemporary icon? A. Brunon-Ernst (Ed.), *Beyond Foucault: New perspectives on Bentham's panopticon. (2013).* (pp. 185–200). Surrey: Ashgate Publishing.

With the passage of time, the panopticon evolved into various types of structures. Each and every type is made to fit the need of the building and its purpose. Structure of panopticon can be applied everywhere and, in every field, as suggested by Lyon. Foucault suggests, if the people in the cells are convicts, then there is no danger of any collective plot, no space for conspiracy, or future planning for any type of crime, no bad influences either; if the inmates are students, then the idea that they are being constantly watched discourage them from indulging in any unacceptable or immoral behavior, no fear of cheating, no chatter, no noise; if they are workers, there is no distraction that will slow them down at work, no theft, no coalition; if they are madmen, there is no fear of inflicting violence on one another; if they are patients, the medicine and personal care for every patient can be increased. Considering the utility of panopticon, Bentham rightly states that this structure enables in segregating actions into disintegrated individualities and rules out the scope of collective effect.[4] Surveillance and cutting off the internet also works in similar manner and discourages collective efforts. Therefore, the whole idea of surveillance is to suppress the liberty of thought, which according to JS Mill is at the kernel of liberty and freedom. The theory of Foucault resonates with the CCTV cameras as the footage of CCTV can be watched from a central tower by the watchmen and also the footage can be stored.

Surveillance through panopticon had been ostensibly practiced during the catastrophe of Plague[5]. The constant gaze and continuous data keeping ultimately went to the Magistrate. The Magistrate had complete control over medical treatment which is based on the register being maintained by the syndic. Everything was noted down whether it was death, illness or any irregularity it was transmitted to Intendants and Magistrates. A similar model of complete lockdown was practiced during the Covid-19 Pandemic as well, where people were not only

[4] Foucault, M. *Discipline and punish: the birth of the prison*. London: Penguin. (1991).
[5] Foucault, *Discipline and Punish* (1991), p. 183 (emphasis in original). Foucault, *Security, Territory, Population – lectures at the college de France, 1977–1978* (2007), pp. 57

worried about the gaze of administration but the people in general were also worried before stepping out of their houses.

Post Panopticon Theories: Deleuze & Guattari, Haggerty & Ericson and Lyon.

The Foucauldian institutions and their way of discipline is shifting to other modes of surveillance in the backdrop of changing socio-technical landscape. Foucault's model fails to cover the electronic layers of the surveillance. Deleuze, also known as the father of post panopticon theory gives surveillance a shift from Foucault's disciplinary societies to the societies of control by Deleuze and Guattari in 1987. But still panopticon is not dismissed entirely, instead panopticon is embedded structurally in the concept of state and governance. Thus, Governance becomes a driving force of surveillance regime[6].

Deleuze argues the new systems of capitalism and globalisation are shaping the world and changing the institutions entirely, turning them into a corporation. He explains surveillance is adopted to channelize discipline in the society and to achieve progress of the society as a whole. It aims at optimal utilization of resources to reach at the government issued goals. The Deleuzian concept of "dividual"[7] puts surveillance on individual as entities rather than treating them as uniform beings. His model focuses on open spaces and access points such as airports, seaports etc. which is different from Foucault's panopticon structure which limits itself to a closed structure such as prisons, hospitals, etc. Deleuze's work on surveillance comes during the time when internet and computers were not yet prevalent as they become so in 1990s and 2000s.

Haggerty and Ericson proposed an entirely different concept and thus attack the panopticon theory. They proposed a concept of "surveillant assemblage" based on the concept of

[6] Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.
[7] Deleuze, G., & Guattari, F. *A thousand plateaus: capitalism and schizophrenia*. Minneapolis: University of Minnesota Press. (1987).

"assemblage" by Deleuze and Gauttari[8]. Their shift of focus is on de-territorialised forms of social control from territorial social control.[9] In this theory, thus, assemblages are discrete flows and limitless phenomena such as people, institutions, knowledge and signs. When such things gather together, they have the capability of dominating the senses that guide the actions of others. Surveillant assemblages are thus "recording machines" that are being used to carry out surveillance. They consider surveillance as nascent, unhinged and lack apparent boundaries or accountable government institutions, so that it can't be challenged and argued by directing the responsibility on single or particular bureaucracies or institutions.

The new post panopticon surveillance has its own characteristics like- it not only focuses on states but also on non-state institutions. Further, the subject matter of surveillance is not humans entirely but are 'entities', the surveillance capacity is being increased exponentially, and surveillance is being made purpose specific such as security, governance, control, profit, and entertainment. Technological possibilities have intensified to carry out surveillance on an enormous scale. It relies on machine though requires a watchman to watch the recording thus making the task less laborious.

Lastly, Haggerty pointed out, debates and studies on surveillance tend to disregard surveillance practices that might be acknowledged as a positive progress[10] (e.g. in science and medicine). The extended 'networked control' should not be professed as a purely negative notion.

Similarly, the inmates are citizens of any country which exercises this power of putting people under surveillance. The extended rights to the government agencies create a central tower from where the watchman is watching the inmates of the digital panopticon without being seen, where their computers are their cells. The blanket order with which Government of India has

[8] Deleuze and Guattari defined assemblages as a 'multiplicity of heterogenous objects, whose unity comes solely from the fact that these items function together, that they *work* together as a functional entity' (Haggerty and Ericson 2000).

[9] Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 97–122). Portland: Willan Publishing.

[10] Haggerty, K. D., & Ericson, R. V. The surveillant assemblage. (2000). *British Journal of Sociology.*

extended this power of putting surveillance in the digital world creates this kind of panopticon but the only difference is that power in Indian context is unverifiable but not visible. Panopticon is a marvellous mechanism through which the power can be homogenized.

The term 'panopticon' is used as a metaphor for 'surveillance'.[11] David Lyon describes that panopticon could still be used to explain how surveillance works and what it does, although in adjusted forms.[12] He claims we can never do away with panopticon historically and the way surveillance industry has evolved after 9/11, it is making presence of 'watching and being watched' perpetual, through all kinds of new technologies.

Problems attached to Surveillance

The surveillance is problematic in various ways; it is slowly depriving people of their rights and making everybody question their lives constantly. It is leading to slow social suicide as social relations are based on trust and trust is the only thing that's not even left between a teenager and his parents. The "dataveillance"[13] is creating a gross discrimination; by keeping tracks of data of people, it is dividing them on the lines of class, race, creed, citizenship, gender and geography. This kind of data collection in 21st century is exacerbating the situation for people on the lines of discrimination, all across the world. Also, surveillance is catering to

[11] There are traditionally two schools of thought in Bentham studies: the authoritarian, which sees Bentham as the master mind of authoritarian state control, and the liberal, which sees him as thinking in terms of rule of law, aiming to promote civil and political rights. There is a deep-seated contradiction in Bentham's writings; Anne Brunon-Ernst, Introduction, in *Beyond Foucault* (2013), pp. 1–2; Schofield (2009), p. 71.

[12] Lyon, D. The search for surveillance theories. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond.* (pp. 3–20). (2006). Portland: Willan Publishing.

[13] Clarke (1988) coined the term dataveillance to indicate that through computational means and digital information, it has become easier for governing actors to trace individuals or groups than was possible with the previous, often expensive and 'heavy' forms of architectural or institutional surveillance. Although databases existed before the computer, they involved equally 'heavy', analogue methods of gathering and storing information.

business-as-usual attitude[14], by collecting their data through Know Your Customer and helping the credit companies to utilize this data for their benefits.

The impact can be explained through the George Orwell's novel "Nineteen Eighty-Four"[15], where he mentions "Oceania", a totalitarian state which can be a dream of Stalin and Hitler. In Orwell's utopia, the only truth which exists is spoken by the state and is based on extreme controls like thought policing. Oceania is full of posters, all with a caption on it saying "big boss is watching you". Orwell's book "Nineteen Eighty-Four" is a classic example of dystopia which is developing due to technological developments and how they are being used to intrude into trivial aspect of people's life. He separates utopia[16] from dystopia on the lines of hedonistic principle. Orwell states in dystopia the notion of 'freedom' and 'pleasure' which we take for granted are taken away through this system of relentless surveillance. Scholars argue that CCTV culture which keeps an individual under constant surveillance is similar to Orwell's vision. In Orwell's book, televisions were becoming popular in British homes and Orwell is showing television as an instrument for brain washing people by the state, which are replaced by computers today. The totalitarian state is living its dream through personified surveillance of 'big brother' who is watching your every move. The big brother is really making the life suffocating and is being used as a drone for spreading their propaganda to indoctrinate it in the thoughts and behavior of people.

[14] David Murakami Wood (editor), A Report on Surveillance Society for the Info Comm by the Surveillance Studies Network, (p- 5-46). (Sept 2006).

[15] George Orwell, Nineteen Eighty-Four, London: Secker and Warburg. (1949)

[16] George Orwell, "Utopia", 1984: He brings to our attention the issues of technological surveillance, torture, continuous low-level war and propaganda and the abuse of language, along with questions about the history up-to- the- present of inequality and its origins. Identify in order to understand where such Orwellian trends might be leading, and how we might stop them.

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 01 Issue 01 KnowLaw

Surveillance in the first world countries

Snowden revealed how the intelligence agencies such as Government connections headquarters in UK and National Security Agency in USA carry out digital surveillance and keep tap on every single activity of people in their country. The illustrated details have led to a series of concerns, which includes public debate and questioning the legality of surveillance, the protection of civic rights, the threat to privacy and liberty of individuals in society, which came under question and the matter went to European Court of Human Rights.

Bedlam ensued after the revelations has brought debate about the public policy on surveillance, the actual policy changes in UK started after the leaks. UK government dealt with surveillance by legislating laws on investigatory powers. The Investigatory Powers Act, 2014[17] legalized 'snooping' and 'hacking' the privacy of individuals on the name of investigation. The agency after Investigatory Powers Act, 2014 is bestowed with unwavering power to track down information about any individual.

After a research conducted by the Cheshire's Deputy Head Constable, Graeme Gerrard[18] revealed that there is one camera for every 32 people in Cheshire. With this being revealed, UK is considered as the "most watched" country of the world. [19] UK is being counted in one of the worst countries in protecting right to privacy along with China and Malaysia, after surveying 36 countries of the world on accounts of their endemic surveillance. A huge group of people call this kind of surveillance as one that suits dictatorship as that of Russia and not democracy or to a namesake democracy as that of China. Snowden's revelations have produced

[17] Ewen MacAskill. 'Extreme surveillance' becomes UK law with barely a whimper. The Guardian. (19 Nov, 2016).

[18] Paul Lewis. You're being watched: there's one CCTV camera for every 32 people in UK, The Guardian, (2 Mar, 2011).

[19] Hintz A. & Dencik L. The politics of surveillance policy: UK regulatory dynamics after Snowden. Internet Policy Review, Vol. 5(3). (2016).

the most outcry in Germany due to its history of mass surveillance after the Budenstag extended even more surveillance powers to the intelligence agencies.

Civil liberty advocates and advocates of privacy in USA have created awareness among the government and society. USA government had been working on relaxing and shaping the policies on the lines of civic rights. Since Snowden's incident, US government is working on its reform policy to tone down its data mining and surveillance activities. But reforms faced a setback after President Trump came into power. Liberal Democrat Lord Strasburger reveals that USA has each and every information that spooks of UK are gathering. In Obama's rule the group of advocates of civil liberties gave 45 recommendations to the government, which put emphasis on eliminating the third party for data mining and also recommended that the NSA and authorities should seek Court's permission to access information. Groups demanded for separate positions of NSA chief and head of US cyber command, which was rejected by the US government. Also, news industry is constantly focusing on Russia as to when is it going to use Edward Snowden for bargaining with Mr. Trump.

But, against a backdrop of fears of terrorist attacks, the advocates for privacy are not able to make much headway. President Obama[20] in his address to the public of USA said that "you can't expect 100 percent security without sacrificing anything". Therefore, the democratic states carrying out surveillance are seeking to strike a balance with the civic rights. Supreme Court of USA has found out that US government has traced down more than 50 terrorist attacks before its successful execution and none of them has been pre-empted through the mass surveillance program being carried out by NSA. Thus, it led way for the framework of GDPR.

The concept of Surveillance in the Legal Framework of India

[20] Barton Gellman, U.S. surveillance architecture includes collection of revealing Internet, phone metadata, The Washington Post, (Jun 15, 2013).

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 01 Issue 01 KnowLaw

Statutory provisions conferring power of surveillance on Indian Government and Administration

The surveillance is mainly carried through intercepting and decrypting the telecommunication messages. The state derives power to carry out surveillance from two most important legislations with regards to digital surveillance namely- the Indian Telegraph Act, 1885 and the Information Technology Act, 2000.

Indian Telegraph Act, 1885 and Rule 419A of Indian Telegraph Rules, 1951 -

The jurisprudence of surveillance can be said to be derived out of the legislation of Colonial era which is the Indian Telegraph Act in this context. Section 5 of Indian Telegraph Act, 1885 confers Central Government and State Governments of India with the power to intercept the messages under instances which are as follows: in the interests of the sovereignty and integrity of India, security of the country, friendly relations with foreign states, decency and morality, public order, defamation of contempt of court, or incitement to an offence.

By exercising the power conferred to the Government under Section 7 of Indian Telegraph Act, in 2007, Rule 419A[21] was added to Indian Telegraph Rules, 1951 framed under Indian Telegraph Act, 1885. The rule provided that orders on interception should only be issued by the secretary in Ministry of Home Affairs. However, an exception was added into it stating that in unavoidable conditions the order could be issued by an officer, not below the ranks of a joint secretary to Government of India. Rule 419A lays down the procedure of interception of any message.

Information Technology Act, 2000 and Electronic Interception -

[21] Rule 419A, Indian Telegraph Rules, 1951.

Section 69 of the Act empowers the controller of certifying authorities to intercept any data circulated through any computer which covers all range of digital devices, systems, network, data, database and software. The authorized person derives their power to intercept from Section 69(1) of IT Act, 2000 read along with Rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Section 69, sub-clause 1 extends this facility to decrypt information as per the directions of controller to a subscriber if controller is satisfied it is necessary to do so in order to protect the sovereignty and integrity of India, security of state, friendly relations with foreign countries, public order, or incitement to an offence. The controller can, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

Sub-Clause 3 provides that any subscriber or any person, if called upon to assist the agency in decrypting the information will do so as per the directions and sub-clause 4 provides for the punishment which may extend to seven years of imprisonment if the subscriber or any person fails to assist the agency when asked.

Section 69 is not backed by any procedural safeguard as Section 5 of Indian Telegraph Act was backed by Rule 419A. The rules issued by Supreme Court for telephone tapping where direction is to be provided by Home Secretary, Government of India, and Home Secretaries of State Governments, whereas as per Section 69, only controller can issue an order for intercepting the information being transmitted from different computers and it cannot be delegated except as per the rules mentioned in Rule 419A.

The operational aspect of Section 69 states that it gives direction to intercept information which is in "transmission" and therefore storing or generating electronic message will not be an offence. The Section is considered to be violative of Article 19(1)(a) which is right to speech

and expression but it is countered by Article 19(2)[22]. Also, it goes against the Right to Privacy under Article 21, which we have already discussed in previous section.

Later in 2009, the lawmakers came out with three separate sections, which are Sections 69, 69A and 69B. The procedure for Section 69 was framed in 2009.

Miscellaneous provisions authorizing surveillance.

Section 3 of the Indian Wireless Telegraphy Act, 1933 prevents possession of wireless telegraphy device without license, if used for intercepting, monitoring and surveillance of communication and considers it as an offence.

An amendment in October 2012 of the Central Motor Vehicle Rules, 1898 added Rule 138A which was concerned about radio frequency and identification tags on heavy and light motor vehicle was authorised. This rule facilitated the monitoring and instant identification by electronic collection toll booths by police or any other authority.

Section 26 of Indian Post Office Act, 1898 authorizes Central Government and the State Governments of India to intercept, detain or dispose a postal article in the course of transmission, on occurrence of national emergency or in the interest of public safety and tranquillity. If there is some confusion around the emergency or on the purpose of public safety, a certificate issued by the Government will be considered as conclusive proof.

Section 91 of the Code of Criminal Procedure, 1973 legalizes targeted surveillance. Any officer in charge of a police station is authorized to summon a person to produce document or anything necessary for facilitating the investigation, trial or any other proceeding. If required, the Commissioner of Police or Superintendent of Police can be asked to detain a document or the required "thing" from the postal or telegraph authority on an order by the Court. Private intermediaries can also come under the ambit of postal or telegraph authority and can be

[22] Article 19(2) of Indian Constitution provides that right to speech and expression can be restricted to protect the sovereignty and integrity of India, security of state, friendly relations with foreign countries, public order, incitement to the offence.

accessed by a police officer at the lowest rank even. On the other hand, Section 92 is more stringent as compared to Section 91 as it empowers only District Magistrate and specific Court to ask for production of required items from postal or telegraph authority.

Loopholes

The Government in this way is moving towards surveillance state and police state. Extending these powers without maintaining any checks may lead to leak of information of every citizen even to bureaucrat at the lowest rank. The major problem with Section 69 is that it is vague and not lucid within its language. Section 69 of IT Act, 2000 seems to have copied its grounds of validity from Article 19 sub-clause 2 of Indian Constitution. The procedures established under Rule 419A has a long and cumbersome chain of hierarchy. This long hierarchy and requirement of following a long chain can lead to creation of loopholes easily and thus can become a threat to the security of the information.

The involvement of third party like any private commercial or any telecom company to intercept data is another threat to this security of data. Therefore, before accepting the rhetoric of national security the Government should come up with stringent security measures and should minimize the surveillance activities to affect the fundamental rights the least.

Evolution of Right to Privacy

Article 12 of Universal Declaration on Human Rights and Article 17 of the International Convention on Civil and Political Rights acknowledge right to privacy as an essential right of all the human beings, across the world. Additionally, India is a signatory to both of the documents which puts emphasis on recognizing “Right to Privacy” as a fundamental right. National Human Rights Commission in India also through its conduct implies that privacy is an essential right for human beings. The principle of privacy is not exclusively prevalent in Indian society but as adopted from the American jurisprudence, the invasion of privacy is categorized as a tort in four ways which are:

1) Unreasonable intrusion upon the seclusion of another

2) Appropriation of another's name or likeness
3) Unreasonable publicity given to other's private life
4) Publicity that unreasonably places the other person in a false light before the public

Right to Publicity is adopted by US government from the second tort. (para 60).

Right to privacy in India has evolved for over 60 years through various cases and judgments. The journey starts from the judgement of Supreme Court in the case of *MP Sharma and Others v. Satish Chandra*, 1954[23], where the defendants prayed to the Court to declare right to privacy as a fundamental right and Court rejected the plea of defendants and held that:

"…a power of search and seizure is, in any system of jurisprudence, an overriding power of the state for the protection of social security and power is necessarily regulated by the law. Thus, there is no justification in making the right to privacy a fundament right when our constitution makers have not added it into the constitution of the country."

In *Kharak Singh v. State of UP*, 1962,[24] the Court held that the police officials are allowed to keep check on repeat offenders physically, which clearly is hostile to the principle of privacy and the Bench denied the right to privacy as part of Article of 21 of India Constitution.
Later in the judgment of *Govind v. State of M.P*.[25], the Apex Court considered the minority view of *Kharak Singh* case and held that right to privacy is entrenched as a constitutional right under Indian Law. The Court laid down three tests for deciding whether right to privacy would be upheld in the given situation, thus concluding that right to privacy is not an absolute right. The three tests were:

a) Important countervailing interests which were superior
b) Compelling state interest test
c) Compelling public interest

[23] MP Sharma and Others v. Satish Chandra, AIR 300, SCR 1077, 1954
[24] Kharak Singh v. State of U. P. (1964) 1 SCR 332: AIR 1963 SC 1295: (1963) 2 Cri LJ 329
[25] Gobind v. State of M. P. (1975) 2 SCC 148: 1975 SCC (Cri) 468

However, the three tests which were laid down in this case were supervening with each other; there was no clear distinction between the terms "state interest" and "public Interest" laid down in this test and they were ambiguous in nature. Also, public interest will always triumph over the right to privacy and will always violate the first condition of test.

The Court firmly declared the 'right to privacy' as a fundamental right but laid down several restrictions which are:

i) Restriction can be imposed on privacy in the interests of the sovereignty and integrity of India, security of the country, its relations with other states, decency and morality, defamation or contempt of court, or incitement to an offence.

ii) Restriction to be imposed for the protection of general interest or interests of Scheduled Castes and Scheduled Tribes.

iii) The right to be restricted if the procedure would require to satisfy the test laid down in *Maneka Gandhi* case[26].

iv) The *Rajagopal* case tests[27]: It lays down three exceptions to the right to privacy a) if person voluntarily push himself into controversy or voluntarily invites or raises controversy; b) if publication is based on public records other than explicitly listed to not be published; and c) No privacy to the acts and conducts of public officials in the context of discharge of their official duties.

The concept of privacy has been evolving through the cases and judgments and its meaning and definition have been gaining more clarity with the passing time. There are certain things that are understood by the Court such as protecting the right of privacy deals with "people and not places". While considering medical privacy, the doctor is entitled to go against the principle

[26] Maneka Gandhi v. Union of India, Supreme Court of India, WP No. 231 of 1977, dated 25-01-1978. The test laid down in this case is universally considered to be that the procedure established by law which restricts the fundamental right should be just, fair and reasonable.

[27] R. Rajagopal v. Union of India, Supreme Court of India, dated 7-10-1994. These tests have been listed as one group since they are all applicable in the specific context of publication of private information.

of privacy if it is to protect some other individual, other than the patient, from a contagious disease as it was held In *Mr. X v. Hospital Z* by Supreme Court. In the context of financial privacy, in the case of *District Registrar and Collector, Hyderabad v. Canara Bank*[28], the Court held that a bank can't disclose information of the transactions of its customer to "any person' who belongs to public office. The Court called it "unnecessary encroachment" because the information would be leaked to anyone and will be open for misuse against the person. The Court and further the legislations that came later prohibited banks from divulging any information to anyone just like that.

The judgement of the case of *MP Sharma v. Satish Chandra* in 1954 and *Kharak Singh v. State of UP* was explicitly overruled by the judgment of 9 judges' bench in the case of *KS Puttuswamy v. Union of India* while India was feeling threatened by the increasing popularity of Aadhar Card and its collection of biometrics of over 1.1 billion people. The Government has made it so popular by making it mandatory to provide Aadhar Card to avail most of the basic services. The threat which came into question was of surveillance on people by keeping track of all the data. The threat which was in question was of misuse of data by public authorities which during trial converted to the question that "whether right to privacy is a fundamental right or not?". In the leading case of *KS Puttuswamy v. Union of India* (2018),[29] Supreme Court, in its judgment, declared that Part III of Constitution of India protects and guarantees right to privacy to all the citizens of India and it is an intrinsic part of right to life under Article 21. This judgement and the following past judgements[30] explicitly state that nothing can be done against the privacy of an individual. Fundamental rights are sacrosanct in nature and therefore, even Government cannot violate it. The judgement also ostensibly states that right to privacy is the basis of other fundamental rights. If right to privacy is protected then right to life and liberty,

[28] Distt. Registrar and Collector, Hyderabad and anr. Vs. Canara Bank Etc. AIR 2005 SC 186

[29]Justice DY Chandrachud, Justice K.S. Puttaswamy (Retd) ... vs Union of India And Ors. (Aug, 2017).
[30] Kesavananda Bharati ... vs State Of Kerala And Anr 1978 4 SCC 225

dignity, equality, worship, etc. can be protected. The Supreme Court in this case took the vision of Government under observations which states that need of Aadhar was to regulate the effectiveness of the scheme of the Indian Government. [Compelling state interest and compelling public interest (test 2 and 3 of *Govind v. State*)].

But ultimately, Court limited the use of Aadhar Card by the following ways:

1) Public authorities will not use the data collected for Aadhar for any other purpose unless permitted by the Court; not even to carry out any criminal investigation. This aspect hinders right to privacy from becoming an absolute right and puts limitations for criminals. (The blanket order stands in contradiction of this point as it proposes other mechanism for deriving data and information).
2) The Aadhar was made a voluntary choice of the citizens and it was not mandatory anymore for the citizens to provide Aadhar number for various purposes, which gives people a chance of exercising their right to privacy as their own individual right. (The blanket order doesn't comply with this principle).

The judgement provides a test for checking the infringement of privacy by the State. The test suggests the ideas to put limitations on the discretion of States. The tests are as follows:

(i) The action must be sanctioned by law;

(ii) The action which is proposed must be necessary in a democratic society for a legitimate aim;

(iii) The extent of such interference must be proportionate to the need for such interference;

(iv) There must be procedural guarantees against abuse of such interference. (para 71).

KnowLaw Journal

Socio-Legal and Contemporary Research

A Publication of KnowLaw

Volume 01 Issue 01 KnowLaw

Measures taken by the government in India

The preventive measures taken by the Government to avoid the menace or misuse of data intercepted are:

- The approving authority has to inform the competent authority about any sort of interception within 3 working days and such interception shall be confirmed within the stipulated 7 days. If confirmation is not provided within the stipulated time such interception shall cease.
- The order will be issued only when acquiring information would seem impossible to obtain from any other reasonable means. The officer is advised to issue the order as the last resort. The orders issued shall specify the name and designation of the officer or the authority to which the intercepted message is to be disclosed under sub-section (2) of Section 5 of the Indian Telegraph Act.
- The order/directions for interception shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.
- The authorized officer to intercept data shall be required to maintain the proper records which would include the intercepted message, the particulars of the officer or authorities who accessed it, the particulars of the person whose data is intercepted, mode and method of the data by which copies are made, duration for which the data is used, the date of destruction of the intercepted data and its copies.
- The service providers shall put in place adequate and effective internal checks to ensure that unauthorized interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception of messages as it affects privacy of citizens and it should also be ensured that this matter is handled only by the designated nodal officers of the company.

- The Central Government and the State Government, as the case may be, shall constitute a Review Committee with its chairman not below the rank of Cabinet Secretary in the case of Central Government and Chief Secretary in the case of State Government and shall review orders within 7 days of its origin. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred above, it may set aside the directions and can order for destruction of the copies of the intercepted message or class of messages.
- The service providers shall destroy records pertaining to directions for interception of message within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy.

Way forward

1) The European Union Regulation of 2016 (para 69)[31] has recognized "the right to be forgotten", which gives an individual a right to get all his information of past erased which he thinks is not relevant and will never be required again. He cannot erase his entire information or information which serves legitimate interest or is correct, relevant, or is still necessary. In *R. Rajagopal v. State of Tamil Nadu*, the Supreme Court suggested right to privacy under Article 21 is a "right to be let alone".
2) Maintaining the spirit of the judgment of *KS Puttaswamy v. Union of India*, the Government should resort to methods which will infringe fundamental rights the least.
3) Any information retrieved through illegal surveillance i.e. the surveillance not approved by the Court should be considered inadmissible in the Court as per the Indian Evidence Act, 1872. Judicial review in every request of surveillance should involve fair suspicion in the proceeding.

[31] Justice DY Chandrachud, Justice K.S. Puttaswamy (Retd) ... vs Union of India And Ors. Para 66, (Aug, 2017).

4) In cases of exception only the surveillance should supersede the right to privacy which again should be approved by the Court on fair evidence of an emergency.
5) The guidelines provided for phone tapping and exercising surveillance judiciously under the judgement of *People's Union for Civil Liberties v. Union of India* (1996)[32] by the Supreme Court of India should be followed and the same principles should hold space in cyberspace too.
6) The surveillance activities should be General Data Protection Regulations compliant. GDPR realizes right to privacy of an individual by establishing rights to access to data, right to be forgotten, right to correction to the data, right to restrict data proliferation without consent and many such rights.

[32] People's Union of Civil Liberties ... vs Union of India (UOI) And Anr. AIR 1997 SC 568