Surveillance In India And Its Legality With Reference To Right To Privacy

Aman Malik

Research Scholar, Department of Law, M.D. University, Rohtak

Abstract

Surveillance of citizens by State and their right to privacy is a controversial issue prevalent in Indian federation. In the twenty first century, a government which is unable to maintain a right to privacy for its citizens that government cannot plausibly establish a democratic regime of equal treatment under the rule of law.[1] India is the world's biggest democracy and one of the countries to acknowledge privacy as a fundamental right in its ruling in 2017. But, recently the government of India gives power of surveillance to ten government agencies including Commissioner of Police Delhi, Central Bureau of Investigation (CBI), Directorate of Revenue Intelligence etc. This action of government leads India towards a path where it might become a police state soon with bureaucrats having access to personal information. This research paper deals with the legal validity of surveillance in India with special reference to fundamental right of privacy. This paper also discusses the analytical history of Supreme Court's engagement with the right to privacy and law relating to surveillance in India. In last suggests valuable suggestions to maintain a balance between surveillance and right to privacy.

Key Words: Surveillance, Privacy, Interception, Intermediaries, Monitoring

A. Introduction

The Ministry of Home Affairs of India on 20 December 2018 empowered ten Central government agencies to monitor, decrypt and intercept information gathered, generated, received or transmitted in a computer. These agencies are CBI(Central Bureau of Investigation), IB(Intelligence Bureau), NCB(Narcotics Control Bureau), CBDT(Central Board of Direct Taxes), RAW (Research and Analysis Wing) DRI(Directorate of Revenue Intelligence), Delhi Police Commissioner and Directorate of Signal Intelligence. This action will bureaucratize the surveillance mechanism. The bureaucratic power will be increased which can be misused because personal data can be collected even without informing the targeted person. A constant sense of being watched creates a drastic effect on communication and curtails individual liberty. There is no clarity about specific grounds on which surveillance request will be approved by authorized officials. This process will turn India into a police state where bureaucrats at the lowest level having access to virtual personal information of every citizen. Approximately two hundred fifty requests for surveillance are approved every day.[2] This approval looks like a rubber stamp as compare to freelance application of mind. One aspect is that

[1] R. Kataria, Right to Privacy: What you need to know?, available at http://www.lawyersclubindia.com/ articles/ Right-to-Privacy-What-you-need-to-know- 03/01/2019 06:20 PM

[2] Tathagata Satpathy, Karnika Seth, Anita Gurumurthy, "Are India's laws on surveillance a threat to privacy", **The Hindu**(New Delhi)Dec.28, 2018

surveillance will be helpful to control the social unrest or threat to National security. But on the contrary it has threat to privacy. So this imbalanced situation needs an urgent and comprehensive solution.

B. The concept of Privacy

Privacy is a minimum and natural requirement of human beings to maintain individual boundaries and to prohibit the entry of others into that area. The right to privacy in India has emerged as a vast concept. It is neither defined in the constitution nor in any statutes. In general words, privacy means a state in which one is not perceived or discomforted by others.[3] Or in other words, it means secret or the state of being free from unwanted interference in individual's personal life or affairs or freedom to be let alone. Privacy implies a right to be free from surveillance by state or other government agencies and to decide whether, when, whom and how individual's personal or organised information is to be exposed.

Black's Law Dictionary states that, privacy includes right to be live alone, right to stay away from unsuitable publicity, right to stay without unjustified interference by people in matters which are not connected with the public.[4]

The Privacy Bill, 2011, provides that individuals shall have a right to his privacy; confidentiality of verbal exchange made to or by him together with his correspondence, conversation over cellphone, telegraph message, postal or electronic mails and other methods of communications; confidentiality of his financial matters, medical reports, legal information and his private as well as family life; protection from surveillance; protection of his honor and data relating to individual.[5]

In broader sense, privacy may be classified as follows:
Physical i.e. limitation on others to observe an individual or circumstances through human senses. Informational i.e. limitation on seeking for or disclosing facts which are not known to others. Decisional i.e. limitation on intervention in decisions that are wholly related to an individual. Dispositional i.e. limitation on to know an individual's state of mind.[6]

The concept of right to privacy in India may be traced out in ancient Hindu text. According to Hitopadesh, some matters like worship, sex and matters relating to family should be protected from disclosure. But the Hitopadesh was related to Positive Morality. So, in ancient Hindu text there was vagueness about right to privacy. In modern time the issue relating to right to privacy was first time discussed in debates of constituent assembly. But it got a reserved support only from B.R. Ambedkar which did't secure the place for right to privacy in Indian Constitution.

[3] https: //www.dictionary.com 03/01/19 5:40 PM
[4] MD S Mondal, Right to Privacy is a Fundamental Right- A Study, available at, http://www.legalservicesindia.com/article/2260/Right-to-Privacy-is-a-Fundamental-Right---A-Study.html 09/01/19 5:15 PM
[5] Evolution of Right to Privacy In India, available at, http://www.legalserviceindia.com/legal/article-276-evolution-of-right-to-privacy-in-india.html, 07/01/2019, 9:00PM
[6] www.businessdictionary.com 04/01/19, 3:20 PM

The question to recognize privacy as a fundamental right arose in *Kharak Singh v. State of U.P.*,[7] in this case Justice Subbarao in his minority opinion stressed that there is a need to recognize the right to privacy as a fundamental right even though it is not explicitly provided in the Constitution. The court refused to give recognition to right to privacy because Constitution of Indian doesn't provide expressly any such right. A similar observation was made by Supreme Court in *M.P. Sharma v. Satish Chandra*.[8] After that, in *Govind v. State of M.P.*,[9] the apex court like recent cases didn't oppose the existence of privacy as a fundamental right. The Supreme Court observed that the right to privacy can't be an absolute right but it has to comply with State interest test. In People's Union for Civil Liberties v. Union of India,[10] the apex court observed that that privacy is a part of fundamental right provided under article 21 of the Indian Constitution. On 24 August 2017 the Supreme Court in case of Justice K.S. Puttaswamy v. Union of India, held that Indians have a fundamental right to privacy.

The acknowledgment of Indian Supreme court to have a right to privacy will take years to understand its implications although some are immediately clear. These changes may affect the government's policy of Surveillance, Aadhaar(centralized database of personal information), DNA profiling bill, the actions of global platform like Facebook, Instagram, WhatsApp and Google.

C. Laws relating to Surveillance in India

In India information technology sector is developing speedily and the most important problem is that there are no particular rules relating to surveillance. But there are some statutes and rules passed by legislature to govern surveillance indirectly. Some of legal provisions are as follows:-

i) Code of Criminal Procedure 1973

Section 91 of Cr.P.C. provides for targeted surveillance. It states that courts and police officer in charge of station have a power to require any document or thing by issuing of summons if it is necessary for investigation, trial or any proceeding under CrPC.[11] According to the provisions of this section law enforcement agencies in India can access to the stored data and request to intermediaries for any information. For example, a notice was issued to a blog bodhicommons.org in February 2013 in the exercise of the power conferred by section 91 of CrPC. In this notice the blog was asked to remove a statement containing defamatory words. This notice also directed to blog bodhicommons.org to give details of registration of URL from where alleged defamatory statement originally made.[12] In addition, section 92 empowers the judicial authorities to order telegraph or postal authority for interception of any parcel, document or thing.[13]

[7] AIR 1963 SC 1295
[8] AIR1954 SC 300
[9] AIR 1975 SCC 148
[10] AIR 1991 SC 207
[11] The Code of Criminal Procedure, 1973, Section 91
[12] Surveillance in India, available at, https://sflc.in/indias-surveillance-state-other-provisions-of-law-that-enable-collection-of-user-information, 05/01/2019, 02:15 PM
[13] The Code of Criminal Procedure, 1973, Section 92

ii) Indian Telegraph Act, 1885

Section 5 clause 2 of the Indian Telegraph Act, 1885 empowers the Central and State governments to intercept telephone or telegraph communication in two situations. Firstly, when public safety or public interest is involved and secondly when the officials authorized satisfied that interception is necessary to safeguard the sovereignty and integrity of India, security of the state, friendly relation with the foreign state or public order etc.[14] Thus, according to section 5(2) surveillance of telephone networks may be conducted only in case of public emergency or in the interest of public safety. But the public emergency and public safety are not defined under this Act. Supreme Court in case of People's Union for Civil Liberties v. Union of India,[15] observed that public emergency means presence of urgent condition or state of affairs calling an immediate action for people at large. The term public safety means condition or state of liberty from threat to public at large. The Government or authorized officials can't resort to phone tapping, if any of the abovementioned conditions are not in existence.

Rule 419A of Indian Telegraph Rules, 1951 which was added in 2007 deals with the procedure, appropriate sanctioning authority, review process and duration for interception. This rule provides that message interception should be done with the previous assent of head or senior officer next to head of authorized security agency. When the competent authority does not confirm the interception within prescribed time than such interception will be allowed by Union Home Secretary or State Home Secretary.[16] All the orders by competent authority for interception of message or class of message should be forwarded to Review Committee.[17]

iii) Information Technology Act, 2000

The I. T. Act, 2000 is a principal legislation in India which provides for the collection, monitoring, interception and decryption of information of digital communications.

Section 69 of I. T. Act, 2000 empowers the government authorities to monitor, intercept or decrypt any information stored, received or transferred in to computer resources. This section provides wider scope as compare to the Indian Telegraph Act, 1885. According to this section the interception is done in the interest of integrity or sovereignty of India, defense of India, state security, relations with other states, public order, to prevent the abetment of commission of cognizable offence relating to the above.[18] This act does not require that interception can occur only in case of public emergency or in interest of public safety. So, the scope of this act is wide as compare to the Indian Telegraph Act, 1885. Section 69 also lays down an obligation for online intermediaries to provide all facilities and technical assistance to the concerned

[14] The Indian Telegraph Act, 1885, Section 5
[15] AIR 1997 SC 568
[16] The Indian Telegraph Rules, 1951, Rule 419 A(1)
[17] The Indian Telegraph Rules, 1951, Rule 419 A(2)
[18] The Information Technology Act, 2000, Section 69

authorized agency.[19] This section also empowers the authorized agencies to collect and monitor information or data for cyber security.[20]

Section 28 of Information Technology Act, 2000 empowers the officials of government to access any data of electronic form during investigation. This section empowers the any authorized officer or the controller of certifying authorities to order the production of information. These officers also have a power to compel the production of information stored in electronic form.[21] The controller of certifying authorities or authorized officers also have a power to access computers and their data in case of suspicion of any contravention relating to chapter six of the Information Technology Act, 2000.[22]

Information Technology (Intermediaries Guidelines) Rules, 2011

Rule 3(7) of Information Technology (Intermediaries Guidelines) Rules, 2011provides that intermediaries like Internet Service Providers (ISPs) or online portals shall provide assistance or information to government agencies when asked to do. The constitutional validity of this rule was challenged before Delhi High Court by Yahoo. But the question relating to its constitutional validity was left open.

Information Technology (Guidelines for Cyber Cafes) Rules, 2011

In exercise of power conferred by Section 87 (2) and Section 79 (2) of the Information Technology Act, 2000 the Information Technology (Guidelines for Cyber Cafes) Rules, 2011 were introduced. These rules provides that in India all the cyber cafes are required to keep record for each login by user and to maintain that record for one year. Rule 7 of Guidelines for Cyber Cafes Rules, 2011provides that authorised officer of registration agency is empowered to examine the computer resource or network established in a cyber café. The owner of the cyber café shall provide the all documents and information which are required by authorized officer.[23] Under the information Technology Act, 2000 cyber café are also considered as intermediaries. So, personal information of an individual can also be accessed through cyber café.

iv) Telecom Licences

In India, the telecom sector in last two decades has seen enormous activity. These last twenty years have offered numerous learning opportunities for government agencies as well as private entities dealing in telecom sector. At present entity concerning telecom services are authorised under Unified Access Services License Agreement to take up measures to facilitate surveillance. For instance, in India all Internet Service Providers and Telecom Service Providers have integrated interception store and forward servers in their networks. All voice call, video call, messages, MMS, GSM and unencrypted data in a way directly falls in

[19] The Information Technology Act, 2000, Section 69(3)
[20] The Information Technology Act, 2000, Section 69 B
[21] The Information Technology Act, 2000, Section 28
[22] The Information Technology Act, 2000, Section 29
[23] Information Technology (Guidelines for Cyber Cafe) Rules 2011, Rule 7

India's Central Monitorig System. Service providers are required to connect their infrastructure with the regional centers of Central Monitoring System.[24]

D. Suggestions

The following are some important suggestions:

1. The decisions relating to surveillance are taken by executive branch which leads towards inherent bureaucratization. So, the request for surveillance should be backed by Judicial and parliament control.
2. The grounds for surveillance have been taken from article 19(2) of constitution and pasted into law. There are no specific ground on which surveillance request is passed. So, the grounds on which authorized officials approves the request of surveillance should be specified.
3. Each request for surveillance should be approved by proper and independent application of mind.
4. The concept of surveillance by government should be harmonized with Citizens fundamental right to privacy.
5. The government should set the clear guidelines for authorities on collection, uses, monitoring and storage of information.
6. The law relating to privacy should be codified which will provides the necessary safeguards for individuals.

E. Conclusion

Indian government has created a legal structure which helps the authorities to carry out surveillance through different legal rules and licence agreements for service providers. It is true that the lawful and targeted surveillance can be a beneficial tool to aid law enforcement agencies to tackle criminal and terrorist activities. But at present the laws in India seems to overextend the surveillance capabilities of government especially in case of individual's right to privacy. Though it is a big threat to privacy but the ultimate aim is to ensure National Security. So, there is a need to maintain a balance between surveillance and privacy. The above mentioned suggestions will be helpful to achieve this goal.

References

1. The Indian Telegraph Act, 1885
2. The Code of Criminal Procedure, 1973
3. The Information Technology Act, 2000
4. Information Technology (Procedure and safeguards for Interception, Monitoring and Decryption of Information) Rules 2009
5. Information Technology(Guidelines for Cyber Cafe) Rules, 2011
6. V. Rajaraman, Introduction to Information Technology, 2nd Edn., PHI Learning Private Limited, Delhi, April 2013

[24] Arindrajit Basu, Gurusabad Grover and Shweta Mohandas, "The Surveillance Industry and Human Righs", The Centre for Internet and Society", India, 15/02/2019

7. Arindrajit Basu, Gurusabad Grover and Shweta Mohandas, “The Surveillance Industry and Human Righs”, The Centre for Internet and Society”, NLSIR, Bangalore, 15/02/2019