1

Balancing National Security and Privacy: Interception of Communication under Human Rights and Fundamental Rights in India

Dr. Teena
Associate Professor,
School of Legal Studies, Apeejay Stya University
teena444parmar@gmail.com

Abstract

The development of information technology to improve the communication for both legal as well as criminal purposes has made it difficult for traditional law enforcement techniques to disrupt the criminal activities. Even though criminals and corrupt individuals use modern information technology as a means of communication, communication interception has emerged as a vital tool in the war against various forms of crime and corrupt behaviour. Information and communication technology has consistently advanced, and this has led to an increase in usage and popularity that has extended beyond legal applications. Criminals frequently exploit information and communication technologies to further their own illegal objectives. Professionalism is a crucial component of every criminal or corrupt activity, making them a crucial weakness. The pivotal point at which law enforcement and intelligence organisations can thwart criminal activity is when two criminal groups are required to communicate information regarding a planned crime. This essay focuses on two issues: first, whether the actions taken by law enforcement agencies violate civil rights and human rights more than they help catch criminals because criminals have switched their operating methods from telecommunication to social media, which is still beyond the reach of law enforcement and intelligence agencies.

Keywords: *Right to Privacy, Interception of Communication, Political Rights, Civil Rights, Right to Life and Personal Liberty, social media, Internet, Information Technology.*

Introduction

To intercept means to halt and take someone or anything that is travelling from one location to another before they

arrive. Wiretapping, also known as interception, is the practise of attaching a listening device to a telephone line in order to listen in on conversations covertly. This practise may also be thought of as the act of removing data or information from a medium before it reaches its intended recipient. In other terms, communication interception refers to the act of preventing or observing communication between a sender and a recipient. The intelligence and law enforcement agencies use the investigative technique of communication interception to safeguard the interests of the country or to prevent or identify crimes in order to control actions that have a direct impact on national security and Integrity. Interception techniques include, for instance, eavesdropping to phone conversations or reading mail before the recipient receives it. Access to communications network data, such as conversations or emails, by the government that has been authorised by law in order to stop criminal behaviour and gathering evidence is known as "lawful interception." Therefore, any law now in effect must permit an interception to be considered legal.

As Per Cambridge Dictionary Interception is defined as "*the action of stopping and catching something or someone before that thing or person is able to reach a particular place*.[1]"

In India, there is still no law governing legal interceptions. India lacks constitutionally valid provisions for legal phone tapping and intercepting communications. The Indian government's law enforcement and intelligence organisations are not subject to parliamentary oversight. Additionally, there is no procedural safeguard being used by law enforcement or intelligence services to protect the subject's right to privacy or any information obtained through such interceptions. The Supreme Court of India also considered whether intercepting communications constituted an infringement on an individual's right to privacy or not. It was decided that public safety must come first and that an economic emergency does not qualify as a public emergency. In response to this lawsuit, the central government amended the Indian Telegraph Rules of 1951 by adding rule 419-A. Because decision-making still lay with the executive branch of the Indian Constitution, the change to the Indian Telegraph Rules likewise failed to eliminate unguided message interception.

The accepted rule in the USA is that getting one of the parties participating in

[1] https://dictionary.cambridge.org/dictionary/english/interception

the conversation's consent before recording a tape conversation is required in order for it to be admissible in court. However, India's legal system is really appalling; evidence gathered through incorrectly assembled interceptions is also admissible in court.

Review of Literature

Privacy is defined by various scholars from different disciplines starting from legal, political, economics, information technology, medical, health and sociological to mention a few. Recently the a few scholars like **O'Neil, Onora (2005)[2], and Nordal, Salvor (2013)**[3] to cite a couple of them. These scholars of the opinion that the privacy is a social concept deeply rooted in the social trust and social obligations.

As a social concept **Nordal (2013**) defines it as "interaction between the person who is enjoying privacy and the person or institution that has particular obligations, the one who is trusted not to interfere, not to share the information with others, and so on"[4]. It is clear from this definition that privacy is relational or social concept not an individual concept. As a relational concept privacy is rooted on two pillars – social trust and obligations.

In India interception is still a very controversial issue and lawful interception is vague process.

Shaik Mohammed Ismail observed that The central government must establish regulations to prevent violations involving communication interception.

Maria Xynou observed that Law enforcement authorities in India require tools to help them combat crime, including all cybercrimes and terrorism in the nation. The many surveillance technologies that are employed by law enforcement organisations can be considered among these tools.

Ms. Sindhu Gurram writes that While monitoring is necessary to track down and stop criminal activity, the right to privacy for each individual is of utmost significance. And neither a person nor a government shall have the authority to intercept except in accordance with the legal process outlined in our constitution and other pertinent legislation.

B. Singh observed that the actual issue is that there is no practical and efficient

[2] O'Neill, Onora (2005). "The Dark Side of Human Rights." In *International Affairs.* Vol.81, No 2

[3] Nordal, S. (2013). Privacy as a Social Concept (Unpublished doctoral thesis). University of Calgary, Calgary, AB. doi:10.11575/PRISM/27435

[4] Ibid., p.80

legislative oversight of India's law enforcement and intelligence organisations. The human rights of every person, including their right to privacy, should always be respected by law enforcement.

Aniruddh Singh writes that the government has no authority to breach someone's privacy, although it may do so in exceptional circumstances, such as when there is a threat to India's security or integrity. In these cases, the government must follow legal procedures.

Statement of the problem

It is crucial to consider whether lawful interception is an effective law enforcement weapon to be employed in this environment given the globalisation, expansion, and corruption of criminal activities and corrupt practises, which is a major source of concern for society.

Objectives of Study

The main objectives of this research are-

1. To understand the procedural aspects of the lawful interception of communication and its adequacy *vis-a-vis* human dignity and right to privacy.
2. To critically analyse the provision of statutes that pertains to the interception.
3. To study the effectiveness of interception in present scenario where a plethora of alternative media i.e., social media/networking of communication are available, which are yet beyond interceptions.
4. To study of misuse of powers by law enforcement agencies under the belief of lawful interception.

Hypothesis

The proposed research paper presupposes that the measures taken by law enforcement agencies (in India) are more violative of civil rights than to nab the criminals due to changing *modus operandi* from telecommunication to social media by the criminals which are yet beyond the interception by enforcement and intelligence agencies.

Methodology

The technique employed in this research is doctrinal, which is exploratory and analytical using numerous secondary sources such books, papers, journals, case reports, and the internet, among others, in order to reach the target.

Legal Framework for Interception

Individual privacy or privacy in private sphere is utilitarian, atomistic, or narrow understanding of privacy, which had relegated privacy to private sphere such as family, marriage, property, personal information and so on. This also had led

to understand the privacy as a right more than obligation or duty. In Indian context it is been inserted within the article in our constitution - right to life (article 21).

Privacy as a social concept is guided by social norms, pattern of behaviours which are expected from the persons, institutions and the society. For example, it there is an obligation from the neighbours that they do not eavesdrop from the window to listen to what the other family members talk, we do not peep on the mobile phones of the fellow passengers in the public transport. Similarly, every society has various social norms around which privacy is been built.

The two pillars of privacy social trust and obligations play vital role protect privacy than any laws. When we share any information, property, space, intimacy, goods and services to the other person or to an institution we trust them that our privacy is respected. Before we sign in to any social site we check their privacy norms, so also, we know the competence of our friends, relatives, spouses, colleagues and even our workplace in retaining our privacy. This is a social trust guarded by social norms. Government more than building surveillance and controlling the individuals for public safety need to build trust among its subjects. Need to make laws to check on various social sites and other institutions have well-guarded privacy norms. It is important for the government to do surveillance in order to stop the criminal activities and the public safety. However, it is more important for the government build trust among people that their privacy is being protected.

The second pillar of privacy is obligation. Privacy is considered as obligation that each one of need to perform in order to respect privacy of each other. As an obligation O'Neill (2005)[5] and Nordal (2013)[6] describe four types of obligations. They are specific perfect obligation (ex: health privacy, professional privacy), specific imperfect obligations (ex: intimacy, friendship), universal imperfect obligations (virtues such as tolerance, care and concern in everyday life is important to uphold privacy in public are held by others special in the context of right to liberty).

Therefore, good privacy laws build up social trust and social obligations which in turn will build better world tomorrow with reduced crimes and increased liberty.

There are numerous laws in India that deals with Interception of Communication in India. Telegraph Act and Information Technology Act 2008 are most vital act for dealing with unauthorised interception of

[5] O'Neill, Onora (1996), pp.187-189 and 202

[6] Nordal, S. (2013), pp.154-159

communication in India and they provide some procedural aspects of Interception also. Indian Telegraph Rules, provides some mandatory requirements of interception under Rule 419A. It specifically says interception of communication can be done by only Central and the state government or any person who is authorised by law for doing so only for the sovereignty, in emergency and in public interest. Furthermore, Section 69 of the Information Technology Act of 2000 gives a controller the power to authorise any government agency to intercept information sent through a computer resource if he determines that doing so is in the interest of India's sovereignty and integrity, the security of the country, the maintenance of friendly relations with other states, or public order in order to prevent incitement to the commission of any crimes that are punishable under the law. The Information Technology Act of 2000's Section 69-B grants the central government the jurisdiction to require any government agency to monitor and gather traffic data or information that is generated, delivered, received, or stored in any computer resources in order to increase cyber security.

The Indian Telegraph Act 1885- Government has right to do lawful interception under the above-mentioned Act.

Section 5(2)-

"On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."[7]

Therefore, it is clear from Section 5(2) of the Indian Telegraph Act that intercepting is only allowed in situations of public emergency or when doing so is

[7] Section 5(2) Indian Telegraph Act

necessary for the protection of the general public. Second, the following conditions must be met with the prior approval of the Central or State Government:

- India's sovereignty
- its integrity
- its security, its relations with other countries
- its public order
- its ability to prevent incitement to commit crimes.

This section is confined only with the telegraph and letters only and any press matter authorised by Central or State government shall not be intercepted or detained unless and until it is prohibited under this Section. If interception done illegally, it is punishable under sections 25, 25A & 26 that provide for imprisonment up to three years, with or without a fine.

Section 25 –"*Intentionally damaging or tampering with telegraphs.—If any person intending— (a) to prevent or obstruct the transmission or delivery of any message, or (b) to intercept or to acquaint himself with the contents of any message , or (c) to commit mischief, damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof, he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both*"[8].

Section 25A-"*Injury to or interference with a telegraph line or post.—If, in any case not provided for by section 25, any person deals with any property and thereby wilfully or negligently damages any telegraph line or post duly placed on such property in accordance with the provisions of this Act, he shall be liable to pay the telegraph authority such expenses (if any) as may be incurred in making good such damage, and shall also, if the telegraphic communication is by reason of the damage so caused interrupted, be punishable with a fine which may extend to one thousand rupees: Provided that the provisions of this section shall not apply where such damage or interruption is caused by a person dealing with any property in the legal exercise of a right if he has complied with the provisions of section 19A (1).*"

Section- 26"*Telegraph officer or other official making away with or altering, or unlawfully intercepting or disclosing messages, or divulging purport of signals.—If any telegraph officer, or any person, not being a telegraph officer but having official duties connected with any office which is used as a telegraph office,— (a) wilfully secretes makes away with or alters any message which he has received for transmission or delivery, or (b) wilfully, and otherwise than in obedience to an order of the Central Government or of a*

[8] Section 25 The Indian Telegraph Act

State Government, or of an officer specially authorized [by the Central or a State Government] to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent Court, discloses the contents or any part of the contents of any message, to any person not entitled to receive the same, or (c) divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same, he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both."[9]

Indian Telegraph Rules, 1951-Rule 419 A

The procedural features of communication interception under the law are covered under Rule 419A. Although the regulation was initially adopted in 1999, it was modified in 2007. It contains the rules for authorising interception. Only when no other reasonable method of information acquisition by competent authority is available will the order be issued.

Information Technology (Amendment) Act 2008-

"Section 69- Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

[9] Section 26, The Indian Telegraph Act.

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.]"[10]

The Information and Technology Act of 2000's Section 69 contains the provision for interception. In accordance with this section, the government or any authorized person, have the authority to do interception of any communication when it is necessary for Sovereignty, integrity, public peace and friendly relations of the any foreign State.

Right to Privacy and Judicial Approach

In the very contentious case of R.M. Malkani v. State of Maharashtra, the Apex Court renders a decision. In this instance, the discussion was taped without the party in question's knowledge and without following the proper legal procedures. Regarding the issue of admissibility, the court acknowledges the technique and refers to it as a "mechanical eavesdropping device." The videotaped evidence was compared to the relevant incident's photograph and was found to be credible even though it had been obtained improperly.

The Apex Court permitted the recorded telephone conversation of Minister's wife and doctor in the evidences even it was against their privacy

The petitioner in N. Sri Rama Reddy vs. V.V. Giri, also known as the Presidential Election Case, claimed that Jagat Narayan had attempted to talk him out of running for office. The taped phone conversation was subsequently presented in court to refute Narain's assertions that the incident never happened. Here, the court used the exchange to demonstrate how a witness could be contradicted if he refuses to answer any inquiry that might call into doubt his objectivity. Additionally, it was noted that this kind of dialogue would serve as direct and primary evidence.

The idea of communication interception was initially developed as a way to gather evidence, but as the field of human rights developed, it evolved into a method of violating particular human rights. The state began to prioritise protecting an individual's right to privacy as the range of human rights grew.

The Supreme Court issued its ruling in 1996, concluding that a case's facts and circumstances determine whether or not

[10] Section 69 Information Technology (Amendment) Act 2008

the right to privacy has been violated. Although the constitution does not have a particular clause about the right to privacy, Article 21 does encompass this right. The Supreme Court also made it clear that phone calls frequently have a personal and private nature. The right to privacy undoubtedly extends to private phone calls made from one's home or place of business. As a result, it was decided that the claimed right cannot be violated other than in accordance with "process provided by law." Following this lawsuit in 1999, the Indian Telegraph Rules of 1951 were changed in 2007 to include a provision for communication interception. The regulations specify who is allowed to tap phones and when. An order for tap can only be made by the union home secretary or his equivalent in the state. Additionally, the government must demonstrate that there are no other ways to obtain the requested information. The high-level committee is required by the court to examine each wiretap's legality.

"Can a person record or tape a discussion of his or her spouse?" the SC asks in Rayala M. vs. Nagphanender Rayala. In this instance, the petitioner asked the court for a divorce from his wife. He supplied a hard drive with the conversation between his wife and others in support of his claim. The trust and chastity between a husband and wife are the foundation of marriage, according to the Supreme Court. Furthermore, secretly recording her telephone contact with friends and family would gravely violate her right to privacy. In addition to being against the law, a husband who secretly recorded a conversation is immoral. Additionally, the court cannot depend on this kind of Evidence.

In another case, Anurima @ Abha Mehta vs. Sunil Mehta, the court determined that recording a discussion without the wife's consent and behind her back constitutes a violation of her right to privacy and of Article 21 of the Indian Constitution.

SOPs laid down by the Home Ministry[11]

"It requires setting up of an internal evaluation cell that will examine a monthly statement from law-enforcement agencies on the fifth of succeeding month. These statements are to detail the authorisation orders received for interception, numbers and emails intercepted including period of interception, number of telephones and emails authorised but not intercepted, etc. The Sops also mention the need for destruction of data and phone-tapping records beyond six months and says for surveillance in remote areas, the competent authority should be informed

[11]https://indianexpress.com/article/explained/interception-of-phone-computer-data-the-law-procedures-and-safeguards-5511051/

within 3 days and permission must be obtained in 7 days, failing which the interception will not be valid."

Right to Privacy Under the Universal Declaration on Human Right 1948-

Human Right are introduced through the Universal Declaration of Human Rights on 10, December 1948. It was most important declaration for the human beings as it protects the rights of individual because we belong to human family. It also emphasized these rights are available to all human beings irrespective of their caste, sex, religion or place of birth. The International Covenant on Civil and Political Rights 1976, is the key foundation of Human Right Declaration and specifically acknowledge the Right to privacy under the Human Right and mentioned under Article 12 as:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[12]

The international Convention and The Human Right Committee Provided their comments on Right to privacy. It further stated that human rights include family, privacy, honour and the reputation under Article 18 and its General Comment 17 and 18. It also demanded that the State surveillance on individual must be under the legal framework and not arbitrary.

Conclusion

This research concludes by stating that surveillance or interception has grown in fructuous due to shifting the base of criminals from telecommunication and interceptable mediums to un interceptable social mediums to pass on the information. Thus, it has led to more breach of right to privacy. So we can say that if the procedure of interception is not according to the provisions of Telegraph Act and Information Technology Act, it is breaching the Article 21 of the Indian Constitution. Article 21 ensures "Procedure established by law" as well as the rights to life and personal freedom. In addition, the International Instruments of Human Right Declaration, which India has ratified, and the 1948 United Nations Convention on Human Rights both recognise the right to privacy as a fundamental human right. It is important to preserve each person's right to privacy, and neither the government nor anyone else is permitted to access it without a court order. Additionally, new communication applications are invented every day in this era of excessive use and abuse of information technology. These technologies are so fleeting that it is difficult to detect them. Consequently,

[12] https://privacy.sflc.in/universal

the conventional methods of interception are only formalities to demonstrate the national security provided by intelligence and police organisations.

Bibliography

1. Article on Interception and Privacy in India VOl IX July 2014.
2. Article by Anirudh Singh "Interception of Communication" 2014.
3. Anurima@ Abha Mehta vs. Sunil Mehta S/o Chandmal, AIR 2016 MP 112
4. A critical Analysis on Telephone Tapping Conversation by Shaik Mohammed Ismail, research journal of computer science and information technology science.
5. Case study on lawful intercept, Tim Ehrlich, Latham and Watkins LLP.
6. https://indianexpress.com/article/explained/interception-of-phone-computer-data-the-law-procedures-and-safeguards-5511051/
7. https://dictionary.cambridge.org/dictionary/english/interception
8. The Indian telegraph Act, 1885
9. The Information and Technology Act, 2000
10. The Surveillance Industry in India, by Maria Xynou
11. Legal Opinion on intercept communication, University of Oxford, January 2006.
12. Legal Opinion on intercept communication, University of Oxford, January 2006.
13. Nordal, S. (2013). Privacy as a Social Concept (Unpublished doctoral thesis). University of Calgary, Calgary, AB. doi:10.11575/PRISM/27435
14. O'Neill, Onora (2005). "The Dark Side of Human Rights." In International Affairs. Vol.81, No 2.
15. People's Union for Civil Liberties vs Union of India and Others 1996 SC 1508 (1996).
16. Rayala M Bhubaneshwar vs. Nagaphanender Rayala, AIR 2008 AP 98, (2008)
17. R. Rajagopalan vs. State of Tamilnadu : 1995 AIR 264, 1994 SCC (6) 632
18. R.M.Malkani vs State of Maharashtra,1973 AIR157 (1972).
19. S. Partap Singh vs. State of Punjab, 1964 AIR 72, (1964)
20. Shri N. Sri Rama Reddy Etc vs. Shri V.V Giri,1971 AIR 1162, (1971)
21. State Of U.P vs. Raj Narain & Ors 1975 AIR 865, 1975 SCR (3) 333