Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7923041

ANALYSIS OF LEGAL PROCEDURE FOR INTERCEPTION OF CALL AND MONITORING OF INTERNET IN INDIA

Nirdesh Deb* and Dr. Sharad Sekhawat**
*Ph.D. Scholar, School of Social Sciences & Languages, Lovely Professional University, Jalandhar, Punjab, India
**Assistant Professor, Department of Government & Public Administration, School of Social Sciences & Languages, Lovely Professional University, Jalandhar, Punjab, India

Abstract:
In the current global age of digitalization and internet connectedness, the daily routines and the targets associated with it have become much easier and more accessible within just a click of a button. But it is very critical to understand at the same time that even technology and its constituent elements associated with it also have some major downfalls because of which the efficiency of the same turns automatically into an illegal tool of malpractices and corruption. Therefore, keeping in view the above scenario, this paper talks about the visualization and analysis of legal procedural methods for maintaining an oversight operational track record of monitoring system of internet in India. Paper puts the concerned viewpoint of fundamental right of right to privacy under the pressing priority of discussion in a perception that can call for the alternative balancing mechanism to protect the right to privacy of all the citizens and at the same time prevent the internet privacy standards of the country from illegal misconducts carrying thereon.
Keywords: - Digitalization, Internet Privacy, Fundamental Rights, Surveillance, Monitoring System, Legal Procedure, Law & Justice.

Introduction:

Internet Monitoring Interception: Contextual Preview

Indian Sub-continent is a developing society with use attendance of internet users on a daily basis and therefore it becomes highly crucial for the legitimate authorities to hold the active control of networks, servers and web activities of all the citizens and the concerned stakeholders for the purpose of ensuring strong protection of the country from unwanted internal and external threats of internet data security and privacy of the citizens irrespective of their personal or official information. Therefore, it is now becoming the need of the hour for the law enforcement agencies to take over the concerned issue of internet monitoring as a pressing priority to intervene and call for the best suggestive mechanisms that can eliminate the malpractices and wrongdoings of illegal internet procedural activities within and outside the country.

Influential Scenario of the Ongoing Uncertainty:

It has primarily been noticed in the very recent cases that have been challenged on the floor of the court about the concerned issue regarding the protection and maintenance of internet privacy standards of the citizens regarding their personal and confidential data. The problem

addressal has been considered several times in the sense that the right to privacy of the citizens is being endangered under this particular threat by various surveillance programs like Centralized Monitoring System (CMS), Network Traffic Analysis (NETRA) and National Intelligence Grid (NATGRID). In majority of the legal proceedings regarding the issue, Software Freedom Law Centre (SFLC) has affirm and claimed that these surveillance systems allow central and state law enforcement agencies to intercept and monitor all telecommunications in bulk of the citizens which is in some or the other way is a violation of the fundamental right to privacy of the individuals. In the testimony of the court proceedings presented, the epilogue drawn from the directions of the centre states that, none of the authority has been given or accorded to any of the administering or enforcement agency for the interception or monitoring of any messages, information or personal data under the three surveillance programs namely known as, CMS, NETRA and NATGRID. It can possibly be argued that, to authorize and examine the interception and monitoring orders issued by the state authorities, there is an unrequired prevalence of deficient supervisory system and the inadequate monitoring appliance under the jurisdiction of law. The appropriate appeal has been generated through numerous institutions to permanently cease and terminate the implementation, execution and operation of the respective surveillance projects, CMS, NETRA and NATGRID, that illegally allows for the bulk collection and analysis of personal data of the citizens resulting into the deterioration of their internet privacy standards and violation of the fundamental right to privacy as a whole.

In the testimony of the court proceedings presented, the epilogue drawn from the directions of the centre states that, none of the authority has been given or accorded to any of the administering or enforcement agency for the interception or monitoring of any messages, information or personal data under the three surveillance programs namely known as, CMS, NETRA and NATGRID. It can possibly be argued that, to authorize and examine the interception and monitoring orders issued by the state authorities, there is an unrequired prevalence of deficient supervisory system and the inadequate monitoring appliance under the jurisdiction of law. The appropriate appeal has been generated through numerous institutions to permanently cease and terminate the implementation, execution and operation of the respective surveillance projects, CMS, NETRA and NATGRID, that illegally allows for the bulk collection and analysis of personal data of the citizens resulting into the deterioration of their internet privacy standards and violation of the fundamental right to privacy as a whole.

All kinds of communication, including phone conversations, WhatsApp messages, and emails, are collected and monitored by CMS, a monitoring system. The artificial intelligence program NETRA, created by the Centre for Artificial Intelligence (CAIR), a division of the Defence Research and Development Organization (DRDO), scans internet traffic for the use of words like "attack," "bomb," "blast," and "kill" in tweets, status updates, emails, and blogs.
In actuality, NETRA is a vast dragnet surveillance system created specifically to watch over the country's Internet networks, including voice over internet traffic passing through apps like Skype or Google Talk in addition to writings in tweets, status updates, emails, instant messaging transcripts, internet calls, blogs, and forums. According to the allegation,

NATGRID is a public-private partnership counterterrorism initiative that will use Big Data and advanced analytics to study and analyze massive amounts of data and metadata about specific individuals from different stand-alone databases belonging to different agencies and ministries of the Indian government. The NATGRID system would allow for the monitoring of train and air travel itineraries, credit card transactions, visa and immigration records, tax and bank account information, and credit card transactions. Various claims have been argued on the floor in the concern that, according to the Supreme Court, it is illegal to intercept or monitor a citizen's financial information or travel arrangements unless it is in the wider public interest and in line with the law. Yet, a response under RTI stated that 7,500 to 9,000 permits were routinely issued every month for the purpose of intercepting and monitoring civilian communications, while the committee responsible for reviewing such permissions only meets once every two months. Therefore, it became critical for the judiciary to come up with the necessary directions stated that, the creation of a permanent independent oversight body, either judicial or legislative, to be responsible for issuing and assessing warrants and orders for legal monitoring and interception in accordance with the Information Technology Act of 2000 and the Indian Telegraph Act of 1885.

The Notion of Surveillance: An Anti-Corruption Tool

Monitoring, data collection, or data interception on an individual by a third party are all examples of surveillance. We are more likely to share our personal and confidential data via the aforementioned methods of communication as a result of technological advancements and an increase in telecommunications and internet users in India, but we are unaware that a third party or an interceptor may be able to collect and monitor our data. Social theorists have envisioned numerous institutional structures and techniques to monitor people' behaviours for both specified and undefined goals throughout history, which is where surveillance as statecraft has its roots. Preserving national security is one specific and acceptable goal, but India's surveillance reform is now unbalanced between privacy rights and national security. However, recent technology advancements have fundamentally altered the architecture of surveillance, where the instruments are now more invasive and harmful to our democratic protections. In order to prevent this issue, India has already passed laws allowing for phone or online monitoring. In its most extreme form, surveillance can be very useful in keeping tabs on criminal activity and threats to national security. In this context, certain authorities and departments are permitted to monitor and intercept the data of others, but the justifications must substantially align with those outlined in the relevant legal provisions. Currently, two laws in India regulate surveillance concerns. The first is The Telegraph Act, 1885, which primarily deals with call interception and forbids third parties from doing so while still granting authorities and justifications for doing so. The Information Technology, 2000, commonly referred to as the IT act of 2000, is another piece of law that deals with surveillance. This law addresses the issue of electronic communication surveillance and offers the essential rules and standards in this area. Because to recent events like Pegasus, which purportedly tracked data of several high-profile Indian people, surveillance is a hot topic. This has forced the government to review its monitoring procedures in order to prevent such occurrences in the future. The right to privacy is a basic right of an Indian person, and illegal monitoring poses a

very significant danger to that right. Threats to privacy implicitly pose a challenge to the basic online rights guaranteed by the Indian Constitution. Furthering this, the federal government is working on laws that will be more regulated and clarified to address cyber concerns and safeguard personal data. It also called for the creation of a data protection authority that would deal with concerns about the privacy and data protection. In light of the precedent difficulties, it is also important to take into account and respect the viewpoints of many other nations and look for solutions to the third-party data interception problem. It is also important to consider the viewpoint of the Honorable Supreme Court of India, as well as the other recommendations and remarks the court provided.

Surveillance Operations in India: Historical Background

Many unlawful spying cases, mostly in Indian politics, have occurred there. Other well-known spying incidents include:

Ramakrishna Hegde, the former chief minister of Karnataka, resigned in 1998 as a result of a phone-tapping controversy. As information about wiretaps on 50 people, including journalists and Janta party leaders, came to light, he resigned for moral reasons. The state police's permission to tap into communications was later made public. In addition to this, unlawful monitoring has also contributed to the downfall of governments. In march 1991, two Haryana police officers were detained for spying outside Rajiv Gandhi's home, which prompted Chandrashekhar to quit as prime minister. Rajiv Gandhi, incensed by the alleged spying, chose not to support Chandrashekhar on the vote for confidence. The infamous Tata Tapes were a significant unlawful spying concern. The disclosure of a significant number of intercepted conversations occurred for the first time with the Tata recordings, which included discussions between businessmen Nusli Wadia, Ratan Tata, and Keshub Mahindra. The illegal and unlawful electronic surveillance made public by The Indian Express revealed Tata's attempts to get the federal government to intervene in a case where the United Liberation Front of Assam (ULFA) was extorting money from tea states, including those owned by the Tata family, in which the ULFA was involved. The CBI investigation into the audio recording leaks was then ordered by Prime Minister I K Gujral, but it was quickly ended for lack of evidence. Some years after the Tata recordings were released, corporate lobbyist Nira Radia's hundreds of talks were exposed in 2008. The income tax agency recorded conversations of Radia with prominent politicians, businesspeople, and journalists during a 300-day period between 2007 and 2009 in relation to the 2G telecom scandal. Ratan Tata was one of the businessmen Radia talked with. Once these tapes were made public, Tata moved to court to ask for a ban on the media from publishing additional recordings of this nature. Illegal spying has often been a problem in Indian history, and the most recent Pegasus virus has called into question the country's current surveillance laws and brought to light the need for revised, stricter regulations. Illegal spying has been shown to pose a severe risk to electronic communication and put people's private security in jeopardy. Along with endangering personal privacy, it might also jeopardize national security, warranting stricter restrictions.

Critical Datapoints:

- Before the Supreme Court intervened in December 1996 (PUCL Vs Union of India SCC 1997), surveillance laws were tolerated without consequence. The Supreme Court then issued a set of rules as protections against the State's unjustified or excessive use of monitoring.
- A Pegasus project examination by an international media consortium found that the Pegasus malware has infected around 50,000 phone lines and their associated devices worldwide.
- The state is given room to act in secrecy due to the ambiguity of these terms, which is made worse by the absence of an oversight system that extends beyond the same department. Using such measures typically undermines the privacy and security of law- abiding individuals themselves, which is a regrettable side effect.
- The Pegasus snooping scandal and widely used surveillance techniques like contact tracing and face recognition technologies without proper protections or regulation have also made the populace suspicious.

Regulatory and Legal Framework:

The rules that were written by the British during colonial times left behind the existing legal framework for surveillance in India. The various police manuals of the various states include surveillance actions by the police as part of their duty since they are a common occurrence. The rules and regulations that follow will make it evident that while the police manuals go into considerable length about the topic of physical surveillance, they are silent on the subject of intercepting phone or internet traffic. The Telecom Act, the Information Technology Act, and the Regulations enacted thereunder, which apply to all security services, not only the police, deal with these matters independently. As different parts of surveillance are covered by different laws in India, there are no set standards for the rules addressing this problem. In order to ensure consistency in the rules and practices of surveillance across the whole nation, this paper argues that it is necessary to have a single piece of legislation that addresses all aspects of monitoring and interception in one location. By its many laws and license agreements with service providers, the Government of India has established a framework of legislation that facilitates the implementation of monitoring by authorities. The Centre for Internet and Society (CIS) agrees that targeted, authorized monitoring has the potential to be an effective tool for law enforcement in combating terrorism and crime. Yet, it appears that many Indian legislation and licensing agreements overextend the government's monitoring powers while insufficiently protecting people's rights to privacy and data protection. The Information Technology Act and its Regulations do have certain measures for data privacy and control some forms of monitoring, but they seem insufficient. This is partially because there is a possibility for misuse because there is now no law in India establishing the right to privacy. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, are a significant step towards establishing a legal framework for data protection in India, but they still don't adequately address concerns about data collection, access, sharing, disclosure, and retention. Moreover, they do not guarantee the creation of a neutral entity, such as a Privacy Commission, to supervise the management of personal data and to handle any breach cases.

Surveillance Regulations: International Viewpoint

United Kingdom:

The UK government has passed a number of laws governing the control of surveillance, including the following important laws:

1. Human rights convention in Europe (ECHS): It outlines essential freedoms and rights for citizens, which the present administration must uphold. The right to respect for one's home, correspondence, and private and family life is guaranteed under Article 8 of this treaty.
2. The Intelligence Services Act of 1994 (ISA): It establishes guidelines for the issuance of authorizations and warrants that provide intelligence services the authority to take action to prevent wireless telegraphy interception.
3. Part 3 of the Police Act of 1997: This specifies the conditions and justifications for approving interference with a person's property and privacy.
4. 2018 Data Protection Act: It controls how personal data is processed. It offers guidelines for proper information management, to which organisations are required to adhere.
5. Regulation for the Protection of Personal Data (GDPR): The GDPR is a law that governs the use of personal information throughout Europe.

Russia:

According to the Russian constitution, a person's right to privacy, to protect personal and family secrets, and to maintain the confidentiality of communications may only be restricted by a court order. Only with the individual's consent may personal data be collected, stored, and used. The Personal Data Law, a significant law pertaining to data privacy problems, was approved by Russia in 2007. It guarantees all sorts of data protection, clarifies what information is considered private, what information can be gathered, and also specifies which organisations are permitted to collect information with the approval of the person in question. The Yarovaya Law, which regulated the telecom and internet sectors in Russia, was passed in May 2014. All telecom firms were required to keep all call and text conversations for a period of six months and to deliver the necessary information to the authorities upon request.

Australia:

The Telecommunications (interception and access) Act of 1979, for example, contains a number of provisions that deal with personal data's interception and storage as well as the legal justifications and circumstances under which a person's data may be intercepted. The Australian government has also passed other laws to monitor surveillance and interception. Another comparable piece of law is the 2004 Surveillance Devices Act. In Australia's Commonwealth, it is a legal act. This law includes authority to assist Commonwealth inquiries into a certain set of crimes. These were the laws of a select few nations; nevertheless, many more nations have approved acts or laws relating to surveillance. Ultimately, we can see that a global standpoint also demonstrates that an individual's personally identifiable information in their country has all the rights to keep their communications confidential, and any type of surveillance or collection of such data can result in a violation of their right to privacy. Moreover, surveillance is also referred to as a very beneficial and advantageous instrument

that, when used in a bona fide manner, can help in detection of threat to the national security, soundness of the country and It is used by several countries to keep tabs on criminals, assisting relevant agencies in apprehending them.

Surveillance Regulations: Indian Standpoint

There are currently two major laws that deal with surveillance in India, and one of the most recent ones involved a spyware programme called Peagasus that is alleged to have collected data on about 300 people without their consent. This has caused the government to reevaluate its laws and policies regarding surveillance.

The Indian Telegraph Act 1885: The intercepting of calls is an important topic covered by the Telegraph Act of 1885. It is a piece of legislation that controls the use of radio, digital data communications, and wired and wireless telegraphy. It grants the Indian government authority to set up, maintain, manage, and supervise any forms of wired or wireless communications on Indian soil. Moreover, it gives government law enforcement authorities permission to monitor phone connections and intercept communications within the parameters outlined in the Indian constitution. The central part of this law that governs call interception is Section 5(2) of the Telegraph Act, which states that if the central or state government, or any other official acting on their behalf, is convinced that it is essential to do so in order to protect the sovereignty and integrity of India, the security of the nation, or to stop any crime, as a result, it is imperative to document in writing that no communications or classes of messages sent or received by telegraph may be forwarded, intercepted, held, or divulged to the government. So, under this legislation, the government has the authority to intercept calls in specific circumstances, such as those involving the sovereignty and integrity of the nation, among others, which is analogous to the limitations on free speech imposed by Article 19(2) of the Indian Constitution. In addition to the aforementioned restrictions, it is claimed that journalists cannot be the target of this legitimate interception.

The Information Technology Act, 2000: The IT Act, 2000 is the official name of this law. Cybercrime and internet commerce are its main topics. This Act was designed to give legal status to information storage and transmission transactions done electronically. It focuses on offences involving a computer or network that is situated in India. Section 69 of the Information Technology Act and the Information Technology (process for protections for Interception, monitoring and Decryption of Information) rules, both of which pertain to surveillance, were passed in 2009 and helped to strengthen the legal foundation for electronic monitoring. Any electronic data transmissions are subject to intercept under this statute. In addition to the limitations set forth in the Telegraph Act and Article 19(2) of the Constitution, Section 69 of the Information Technology Act expands the use of surveillance by allowing it to be used to look into criminal activity.

The Personal Data Protection Bill, 2019 was a bill that the Indian government introduced in addition to these two enabling laws. The law establishes a data protection authority and aims to protect personal information about persons. This law calls for the processing of personal data by the government, Indian corporations, and international businesses that conduct business in India. Personal data is any information that, after processing or decryption, may be used to determine the identify or identification of a certain person. But, at present this law is being

reviewed by a Joint Parliamentary Committee and as per the latest remarks the experts are demanding that Data protection bill is weighted in the advantage of the government and it is shifting attention away from individual privacy. The Joint parliamentary committee has adopted its report after two years of protracted deliberation, and in this report, they have offered many revisions and improvement including the recommendation of changing its name to 'Data Protection Bill' eliminating the word 'personal'. The research suggests that both personal and non-personal data should be governed by the same agency. India, a growing nation, need additional laws and limits to protect people's privacy and prevent any kind of unauthorized monitoring.

Legal Jurisdiction & Judicial Proposition:

It has been considerably noticed and contemplated that The Supreme Court has stated that the government is entitled to withhold predefined data, information and details if it falls under the significant restrictions and reasonable limitations of Article 19 clause 2, but that if the state attempts to infringe on a citizen's fundamental rights, this cannot be acknowledged, and that the Union of India should not be placed in a precarious and difficult spot when this occurs. Thus, from many of the mentioned cases, it is clear that the Supreme Court believes that illegal surveillance is unquestionably a threat to the right to privacy and has previously advised the Indian government not to infringe on a citizen's fundamental rights unless they are justified and in accordance with Article 19(2) of the Indian Constitution. It has also stated that if surveillance appears to be a reasonable option, then the relevant authorities must maintain adequate records and logs of the data.

Strategic Suggestions: A Pressing Priority

There should be a single policy statement, proposal or surveillance and interception manual that contains the rules and regulations covering all types of surveillance in order to prevent different standards being implemented for various elements of surveillance and in various regions of the nation. This might be effective for optimizing the overall monitoring system as well as detecting legal issues. Yet, it takes a tremendous amount of work at the legislative level and is easier said than done. This is due to the fact that under India's Constitutional system, maintaining peace and order is a state responsibility, and each State's police force is governed by its own State government. Due to the States' independence in their ability to deal with the police apparatus, it would not be able to pass a single law that addressed all areas of monitoring. Getting both the Central and State governments on the same page is the main challenge in establishing harmonization because of the aforementioned legal and constitutional complications. The State governments will still be able to act whatever they see fit, even if the Central government alters the Telegraph Act and the IT Act to bring them into compliance. Thus, it appears that a double strategic approach, consisting of (i) issuing a National Surveillance Policy that addresses both interception and general surveillance, and (ii) amending the central legislations, such as the Telegraph Act and the Information Technology Act in accordance with the National Surveillance Policy, is the best course of action to achieve harmonization. It is envisaged that state governments would accept the tenets expressed therein and alter their own legislations dealing with interception to comply with the National

Surveillance Policy once a national surveillance policy based on empirical evidence and the most recent criminology theories is released.

Way Forward:

Being one of the world's major democracies, our responsibility to uphold national security as well as the rights of our citizens must coexist. Since the introduction of technology and methods of digital monitoring, national security and privacy have typically been seen as opposing goals. But, preserving people' information is now as crucial. The optimum moment to start considering safeguarding national security as a component of protecting citizen privacy and information may be now. Currently, legislation is moving in a direction that prefers to weaken or exempt privacy practices towards citizens rather than putting in place privacy-respecting practices. This is evident in the amendments made to the IT Act 2000 through the IT Rules 2021 and the extensive exemptions to government and allied agencies in the proposed Data Protection Bill 2021. Using such measures typically undermines the privacy and security of law-abiding individuals themselves, which is a regrettable side effect. In order to assist law enforcement, the IT Rules, for instance, impose originator tracing, which might weaken encrypted communication and introduce weaknesses into other systems that could be readily abused by dishonest characters.

Conclusion:

Surveillance is a beneficial means of preserving cohesiveness and for the nation's safety, but if done by foreign entity or unapproved individuals can generate a great deal of challenges for the general population and may also actually impact the well-functioning of the nation. Hence, under this situation, stricter government regulations on the protection of citizen rights and the privacy of personal information are urgently needed. The Peagasus case demonstrates that even the government may occasionally violate a person's fundamental rights out of political expediency. If the government can do this, imagine what a third party or an individual could do. It is obvious that new laws must be passed in order to place more sane limitations on unauthorized monitoring and data collecting. It is clear that no authority exists to protect data or to look into those who unlawfully collect, use, or keep personal or non-personal information about people. There are a number of laws in other countries, similar to those in Russia, that grant the government the authority to store a person's personal information. These laws can lead to less openness and more instances of legal rights violations. As a result, we require more extensive and comprehensive legislation in our nation. Given that a large portion of the population in India uses digital devices, and that number is growing daily, it is the responsibility of the government to ensure that the information citizens share is safe, secure, and out of the hands of unauthorized parties. Thus, In order to strike a balance between personal privacy and national security, we think that the campaign for comprehensive surveillance reform for targeted monitoring will spark a discussion about setting the groundwork and foundations for new legislative changes for other types of surveillance.

Bibliography:

1. Vipul Kharbanda (Aug, 2015). "Policy Paper on Surveillance in India". The Centre for Internet & Society. https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india

2. Kamesh Shekhar & Shefali Mehta (Feb, 2022). "The state of surveillance in India: National security at the cost of privacy?". Observer Research Foundation. https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/#:~:text=Under%20the%20legal%20grounds%20of,with%20international%20governments%2C%20integrating%20public

3. Mr. David Kaye (Feb,2019). "The Surveillance Industry and Human Rights". Software Freedom Law Centre. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/SFLC_IN.pdf

4. Ira S. Rubinstein, Gregory T. Nojeim, and Ronald D. Lee (2014). "Systematic government access to personal data: a comparative analysis". International Data Privacy Law. Doi: - https://doi.org/10.1093/idpl/ipu004

5. P. Arun (December, 2016). "Surveillance and Democracy in India: Analysing Challenges to Constitutionalism and Rule of Law". Journal of Public Affairs and Change, Vol. I No.1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=29