

POWER OF SURVEILLANCE-BOON OR BANE

Dr. Ashwini Vinod Ingole¹

INTRODUCTION-

Privacy has been most cherished value of human life. If someone tries to intervene into it, we as human do our best to safeguard our privacy. But what if the infringement of privacy is in the interest of community or nation as whole? This conflict of interest has existed since ages in our civilizations and law has tried its best to balance these conflicting interested through several dynamic adaptations.

The recent Pegasus issue has exposed the vulnerability of human privacy. Pegasus is a spyware developed by NSO Group, an Israeli surveillance firm that helps spies hack into phones. In 2019, when WhatsApp sued the firm in a U.S. court, the matter came to light. In July 2021, Amnesty International, along with 13 media outlets across the globe released a report on how the spyware was used to snoop hundreds of individuals, including Indians. While the NSO claims its spyware is sold only to governments, none of the nations have come forward to accept the claims². These technological advances necessitate us to look at the concept of surveillance in detail and understand it from legal point of view as well. The author has taken the same tread and has analyzed the concept of surveillance along with its legal implications. At the end, the author has attempted to summarize the contemporary development from legal analytical point of view and give some practical recommendations to be implemented in near future.

SURVEILLANCE-

1. MEANING AND OBJECTIVE-

The concept of surveillance is very old. It means in normal parlance, it means keeping watch over a person or a property. It also means supervision. The dictionary meaning from legal perspective is “the careful watching of a person or place, especially by

¹ Assistant Professor ,Marathwada Mitra Mandal's Shankarrao Chavan Law College

² Pegasus Surveillance, The Hindu (26/09/2021) , available at <https://www.thehindu.com/topic/pegasus-surveillance/>, last seen on 26/09/2021

the police or army, because of a crime that has happened or is expected"³. The tool of surveillance is adopted by the Government for several purposes like to detect the disease at particular locality within state, to prevent the occurrence of crime by having surveillance of existing criminals, to collect intelligence for national security purposes etc.

2. SCOPE

Many people have security systems that protect their homes and businesses, meaning that they are aware of some form of overt and mechanical surveillance. However, there are several types of surveillance that go beyond stationary cameras and alarm sensors. The practice of surveilling is only in part video and security, and it extends into the arena of covert tactics and investigations⁴. If analyzed properly, there are following basic forms of surveillance⁵-

- a. Interviews – For a missing person investigation, interviews are paramount to understanding the subject. Most often family members, co-workers, friends and neighbors will be talked to in an attempt to discover information and insight.
- b. Physical observation – Physical observation is common for spousal investigations. This type of surveillance involves the actual viewing and following of a subject, and it may include stakeouts, disguises and multiple investigators.
- c. Electronic – Electronic monitoring is often the tool of choice among investigators. This involves the use of electronic equipment to record and document activity. For instance, wiretaps, radios and televisions are common tactics.
- d. Technical – Technical surveillance can also be referred to as A/V surveillance. This involves the use of audio and visual equipment, like digital cameras, to record and document investigations.

Beyond the forms of surveillance, there are also different methodologies which are as follows⁶-

- a. Covert versus overt- Covert practices are common in insurance or spousal investigations. They require the agent or investigator to remain undetected. Overt is when the surveillance is apparent, like in home security systems.

³ Available at <https://dictionary.cambridge.org/dictionary/english/surveillance>, last seen on 23/09/2021

⁴ Understanding Different Types of Surveillance, available at <https://www.investigations.com/security-trends-analysis/different-types-of-surveillance/>, last seen on 23/09/2021

⁵ Ibid

⁶ Ibid

- b. Mechanical versus human- Mechanical methods use cameras, voice recorders and other recording devices to ensure a digital or hard copy file for the results of the inquiry. A human investigation is when devices are ignored in favor of a direct source of information. However, most firms will use both mechanical and human methods.
- c. Stationary versus mobile- Stationary investigations involve staying in the same location and watching the subject. Mobile investigations are the opposite, where the subject is followed from place to place.

The operation and characteristics of most surveillance systems are relatively complex, but every surveillance system can be described with respect to the following nine basic attributes⁷:

- a. Simplicity refers to the system's structure and ease of operation.
- b. Flexibility is the ability of the system to adapt to changing information needs and operating conditions with minimal additional cost.
- c. Data quality is the completeness and validity of the data collected through the system.
- d. Acceptability is the willingness of persons and organizations to participate in the system, including those who operate the system, report cases of the disease, or use the data.
- e. Sensitivity is the proportion of cases of a disease detected by a surveillance system and the ability of the system to monitor changes in the number of cases over time, such as outbreaks.
- f. Predictive value positive is the proportion of cases reported through the system that are accurately diagnosed instances of the disease under surveillance.
- g. Representativeness is the extent to which the system accurately describes the occurrence of the disease over time and its distribution in the population by place and person.
- h. Timeliness reflects the delay between steps in a surveillance system and availability of information for control of the disease under surveillance when needed.
- i. Stability is the ability of a surveillance system to collect, manage, and provide data without failure and to be operational when needed.

⁷ Attributes of Surveillance System, available at https://www.cdc.gov/training/SIC_CaseStudy/Attrib_Surv_Sys_ptversion.pdf, last seen on 23/09/2021

Though these are attributes of disease surveillance, they are commonly applicable to all types of surveillance.

Thus, it can be seen that the scope of tool of surveillance is very wide and it can cover each and every type of human activity and feeling. The surveillance in physical form has always been in vogue for several objectives and it has been employed by governments and private entities since decades for serving their multiple purposes. The digital revolution has brought with it enormous power to the tool of surveillance which is harnessed to the greatest extent by each and every entity which employs it. The electronic surveillance has the global reach from a remote geographical location and this omnipotent presence of electronic surveillance tools has created the question whether the tool of surveillance is boon or bane.

INTERNATIONAL COMPARATIVE LEGAL PERSPECTIVE

Technological developments since the Cold War, during which espionage and the monitoring of civilians was widespread, has increased the intrusiveness and power of surveillance. The ability to monitor the communications of entire groups and nations on a mass scale is now a technical reality, posing new and substantially graver human rights issues. Recent reforms of surveillance laws undertaken across political systems with significant checks and balances show how easily surveillance capabilities can outstrip the ability of laws to effectively regulate them. In nondemocratic and authoritarian systems, the power gained from the use of surveillance technologies can undermine democratic development and lead to serious human rights abuses. Opposition activists, human rights defenders, and journalists have been placed under intrusive government surveillance and individuals have had their communications read to them during torture. State agencies are also utilizing technologies used for surveillance for offensive and military purposes as well as espionage⁸.

The United States of America has been considered as one of the most democratic countries; however, it has been criticized on account of its greatest abuse of surveillance tools and laws and weakening of civil liberties. If we look at the historical background of surveillance powers utilized by American Government, we will find that in the two decades following the establishment of the United States National Security Agency (NSA) in 1952,

⁸ *The Global Surveillance Industry*, A Report by Privacy International, July 2016 available at https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf, last seen on 23/09/2021

there was very little regulation stipulating how government agencies could collect information on individuals. That changed in 1973, when the Supreme Court ruled that warrants were required for domestic intelligence surveillance. Two years later, the Senate's Church Committee investigation found that the NSA had been illegally spying on anti-war protestors, activists, and political opponents. The committee prophetically noted that "no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide."⁹

It was against this backdrop that the two main legal authorities regulating U.S. spy activities came into effect – the Foreign Intelligence Surveillance Act of 1978 (FISA), and Executive Order 12333, signed by President Reagan in 1981¹⁰. Then, in the wake of the 9/11, the Bush administration acted swiftly to implement a host of legal and policy changes in the name of national security. Their lasting effect, however, has been to establish a landscape of surveillance on U.S. citizens. Section 215 of USA Patriot Act (2001) enabled and strengthened many forms of dragnet government surveillance, allowing the CIA to access a wide range of sensitive information on U.S. citizens. This included phone and email communication, Internet use, bank and credit reporting record, school records, and details of criminal investigations and grand jury proceedings¹¹. A key element of the NSA "President's Surveillance Program" – as revealed by the Snowden leaks in 2013 – was Stellarwind, the code name for a program that allowed the NSA to monitor call and text metadata of U.S. citizens and tap any international calls that included a U.S.-based caller. Millions of electronic communications were scanned on a daily basis via AT&T's facilities and satellites to search for associations with the terrorist group Al-Qaeda, and leads were forwarded to the FBI. A classified internal FBI document from 2006 revealed there was no evidence that Stellarwind was successful in preventing terrorism. The program was shut down in early 2019¹².

Such type of intrusive surveillance programs by U.S. Government were carried on regular basis under each and every President. Every Government tried to justify the usage of power of surveillance in the name of national security and prevention of crime. However,

⁹ United States of Surveillance, *The Privacy Issue (Guides)* (22/01/2020), available at <https://theprivacyissue.com/government-surveillance/united-states-of-surveillance-us-history-spying>, last seen on 23/09/2021

¹⁰ Ibid

¹¹ Ibid

¹² Ibid

whenever called to do so, every government authority and personnel responsible for the same failed to substantiate the stated justifications for surveillance programs¹³.

Apart from the U.S. landscape on surveillance, if we analyze the E.U. laws on surveillance and data protection, we will find the roots are more deep and intrusive. The state surveillance system was most widely used by Nazi Germany. As the time progressed and with the post-World War II developments, laws started taking control of State surveillance systems used on European soil and concerns about unnecessarily intrusive census questions led to a landmark 1983 Federal Constitutional Court case that declared the right of “self-determination over personal data” as a fundamental right. That became the cornerstone of the E.U.’s views today¹⁴. The current E.U. law i.e. General Data Protection Regulation lays down rules for the protection of natural persons with regard to processing of personal data and rules relating to free movement of personal data¹⁵.

Europe has been good about enacting protections on privacy that tend to apply to all sectors of the economy, whereas in the U.S. laws apply to certain sectors (such as healthcare) more than others. But, especially after Cambridge Analytica’s Facebook data breach and the Equifax hack raised awareness of data privacy in the first half of this year, Americans have expressed interest in the government taking more action¹⁶ Further, it has to be noted that ever since Edward Snowden’s revelations about the U.S. National Security Agency’s intelligence collection programs inspired Max Schrems’ campaign to end Facebook’s data transfers from Europe to the United States, U.S. foreign surveillance laws have been under the microscope in European courts. They have not been viewed favorably, leading the Court of Justice of the European Union (CJEU) to abruptly terminate two successive transatlantic data transfer arrangements – the Safe Harbor Framework and the Privacy Shield Framework¹⁷.

¹³ Ibid

¹⁴ *The GDPR is just the latest example of Europe’s Caution on Privacy Rights. That Outlook has a disturbing history*, The Time, available at <https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>, last seen on 23/09/2021

¹⁵ The General Data Protection Regulation, available at <https://gdpr-info.eu/art-1-gdpr/>, last seen on 23/09/2021

¹⁶ Ibid

¹⁷ *U.S. & European Surveillance Law Regime: Time to Adjust the Contrast*; About Intel: European Voices on Surveillance, available at <https://aboutintel.eu/us-european-surveillance-law-regimes-contrast/>, last seen on 23/09/2021

Thus, it can be seen that the power of surveillance is used and abused as per the political discretion at international level. Though Europe and the U.S.A. are using the power of surveillance with same state objective, the interrelation between these two is marred by hostility and no nation wants a spy against itself even if it is spying on others.

LAWS IN INDIA

Recently, a global collaborative investigative effort has revealed that, at least 300 individuals in India were potentially identified for targeted surveillance using sophisticated spyware called Pegasus. However, the government of India has claimed that all interception in India takes place lawfully¹⁸. These current developments inspired the author to analyze the legal structure in India dealing with the laws of surveillance and privacy.

Communication surveillance in India takes place primarily under two laws — the Telegraph Act, 1885 and the Information Technology Act, 2000. While the Telegraph Act deals with interception of calls, the IT Act was enacted to deal with surveillance of all electronic communication, following the Supreme Court's intervention in 1996.¹⁹

If we peruse the provisions of the Telegraph Act, Section 5(2) of the Act reads: “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 authorized 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...²⁰” Thus, it can be seen that the law itself has restricted the power of interception enjoyed by the Government

¹⁸ Surveillance Laws in India & Privacy, Drishti IAS, available at <https://www.drishtias.com/daily-updates/daily-news-analysis/surveillance-laws-in-india-and-privacy>, last seen on 23/09/2021

¹⁹ *Explained: The laws for Surveillance in India & Concerns over Privacy*, The Indian Express, 03/08/2021, available at <https://indianexpress.com/article/explained/project-pegasus-the-laws-for-surveillance-in-india-and-the-concerns-over-privacy-7417714/>, last seen on 20/09/2021

²⁰ Ibid

only in certain situations like in the interest of the sovereignty and integrity of India, the national security and so on. These restrictions are same as that of reasonable restrictions mentioned in Article 19 (2)²¹ of the Indian Constitution.

Significantly, even these restrictions can be imposed only when there is a condition precedent — the occurrence of any public emergency, or in the interest of public safety. Additionally, a proviso in Section 5(2)²² states that even this lawful interception cannot take place against journalists. “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 subsection.”²³

Section 69 of the Information Technology Act and the Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were enacted to further the legal framework for electronic surveillance. Under the IT Act, all electronic transmission of data can be intercepted. So, for a Pegasus-like spyware to be used lawfully, the government would have to invoke both the IT Act and the Telegraph Act. Apart from the restrictions provided in Section 5(2) of the Telegraph Act and Article 19(2) of the Constitution, Section 69 the IT Act adds another aspect that makes it broader — interception, monitoring and decryption of digital information “for the investigation of an offence”. Significantly, it dispenses with the condition precedent set under the Telegraph Act that requires “the occurrence of public emergency of the interest of public safety” which widens the ambit of powers under the law²⁴.

CRITICAL EVALUATION

The adoption of mass surveillance technology is the matter of contention across the globe. According to the Council of Europe Commissioner for Human Rights, “[i]t is not only the actual use of these measures against given individuals that infringes the right to privacy but also their potential use and/or the mere existence of legislation permitting their use”.²³ This in no way means that other fundamental rights are not equally affected. The EP resolution highlighted this when referring to other affected fundamental rights, in particular

²¹ Article 19 (2), The Constitution of India, 1950

²² The Telegraph Act, 1885

²³ Supra at 18

²⁴ Ibid

“freedom of expression, of the press, of thought, of conscience, of religion and of association, [...] the presumption of innocence and the right to a fair trial and non-discrimination”²⁵.

If we consider the Indian landscape of laws relating to surveillance and privacy, in 2012, the Planning Commission and the Group of Experts on Privacy Issues headed by former Delhi High Court Chief Justice A P Shah were tasked with identifying the gaps in laws affecting privacy in India. On surveillance, the committee pointed out divergence in laws on permitted grounds, “type of interception”, “granularity of information that can be intercepted”, the degree of assistance from service providers, and the “destruction and retention” of intercepted material, according to a report by the Centre for Internet & Society²⁶.

In the year 2019, the Indian Supreme Court declared in very specific terms that the right to privacy is fundamental right²⁷. After this landmark judicial pronouncement, the landscape of laws relating privacy in India changed to greater extent and the laws relating to surveillance need an overview all together. However, it has also been made clear that the right to privacy is not absolute. Hence, this pronouncement has safeguarded the power of surveillance granted to the Government only in exceptional circumstances. Thus, this new emerged scenario the Government expected to behave responsibly to while exerting the power of surveillance.

CONCLUSION

Every power has two sides. It can be used to the fullest benefit of the society or it can be abused to the detriment of society and for the breach of human rights. Power is surveillance is one of such powers which empower the Government to interfere into personal sphere of human lives. However, it must be understood that Government has the responsibility of maintaining law and order in the society and prevent the threats to national interest and security. So it must be endowed with certain overriding powers to fulfill its societal protection agenda. However, it must always remember that fundamental rights need to protected and balanced along with societal interests.

²⁵ *Surveillance by Intelligence Services: Fundamental Rights Safeguards & Remedies in E.U.*, Report by European Agency for Fundamental Rights, 2015, available at <https://www.statewatch.org/media/documents/news/2015/nov/eu-fra-2015-surveillance-intelligence-services.pdf>, last seen on 24/09/2021

²⁶ *Supra* at 23

²⁷ *K.S. Puttaswamy v. Union of India (Aadhaar-5 Judge)*, (2019) 1 SCC 1

If the Government uses the legal tool of surveillance in balanced manner, it can successfully capitalize the beneficial power of surveillance for the overall benefit of the nation and it can be boon, However, if it fails to recognize this fundamental truth then it will have to tackle the adverse consequences of this power of surveillance and it will prove to be bane. Hence, it can be well concluded that power is surveillance can prove to be both boon and bane as per the usage by the authority.