Page 1011 - 1019 **DOI:** *https://doij.org/10.10000/IJLMH.112002*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 5

2021

Surveillance Laws in India in light of the Pegasus Project

SHRESHTHA MENON[1]

ABSTRACT

The issue of surveillance law in India and its limitations has gained traction after the recent Pegasus incident where an Israeli-developed malware called Pegasus was used to target and steal information from the phones of several individuals. Reports claim that the software surveyed approximately 1,400 phones worldwide. This incident along with many other instances has raised concerns among citizens regarding unauthorized surveillance and breach of cyber security. This paper highlights and analyses the regulatory legislation regarding surveillance laws in India. The two main provisions are the Information Technology Act, 2000 and the Indian Telegraph Act, 1885. The paper discusses the threat such unauthorized surveillance poses to the right to privacy which is enshrined under Art.21 of the constitution. The capacity of the government surveillance as per the license agreements. The paper also analyzes the recent judgments of courts regarding surveillance and the proposed Personal Data Protection Bill, 2019. The paper finally discusses ways to improve the inadequate data protection policy.

Keywords: *Information Technology act, 2000; Right to Privacy, Indian Telegraph act, 1885*

I. INTRODUCTION

In July 2021, Amnesty international and other organizations released a report investigating the software which was used to infiltrate the phones of human rights activists and journalists across the globe. The investigation revealed a spy software called Pegasus which was used to strategically hack phones. The software was created by NSO group, an Israeli surveillance firm. The investigation began after the discovery of the targeting of an Amnesty International staffer and a Saudi activist[2]. The report attributed such attacks to the NSO group by tracking suspicious domain names used and other network infrastructure used to deliver the attacks. The software can hack all recent iOS versions up to iOS 14.6. Following the report, the NSO group

[1] Author is a student, India.

[2] Amnesty International. 2021. *Forensic Methodology Report: How to catch NSO Group's Pegasus*. [online] Available at: <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> [Accessed 30 September 2021].

 [ISSN 2581-5369]

has claimed that the allegations levied against it are false and misleading. They further stated it only sells its software to the government for national security purposes[3].

Through forensic analysis, the report has revealed that 155 people in India were targets by the software[4]. The list includes journalists, businessmen, and political leaders, leaders of the opposition party, lawyers, and officials of the election commission, foreign diplomats, and intellectuals[5]. The Ministry of Electronics and Information Technology on its part has denied all claims of illegal surveillance[6]. However, neither NSO group nor the Government of India have outright denied selling or purchasing the software.

The Information Technology Act, 2000[7] and the Indian Telegraph Act, 1885[8] are the two main legislation for intercepting data and telephones. The government of India claims that all interception is done through the competent authority as per the rules of IT (Procedure and Safeguards for Interception, monitoring and Decryption of Information) Rules, 2009. The competent authority, the Union Home Secretary or State Secretaries in charge of the Home Departments, can issue orders for interception, monitoring and decryption. However, the current rules and license agreement seem to give the government room to maneuver around the limitations imposed upon it through the provision. Such latitude can endanger an individual's right to privacy and data protection. The report has revealed gaping hole in the legislature and its potential for abuse. The lack of accountability is a growing concern among civil rights groups. Such interception should not be carried out to suppress freedom of press .Therefore, in light of the Pegasus project, this paper aims to analyze whether the prevailing surveillance laws are adequate to safeguard the citizen's right to privacy.

(A) Research Methodology

The research methodology adopted for this project is Doctrinal research. A doctrinal research

[3] NSO Group. 2021. *FOLLOWING THE PUBLICATION OF THE RECENT ARTICLE BY FORBIDDEN STORIES, WE WANTED TO DIRECTLY ADDRESS THE FALSE ACCUSATIONS AND MISLEADING ALLEGATIONS PRESENTED THERE.*. [online] Available at: <https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/> [Accessed 30 September 2021].

[4] The Wire. 2021. *Pegasus Project: 161 Names Revealed By The Wire On Snoop List So Far*. [online] Available at: <https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance> [Accessed 30 September 2021].

[5] the Guardian. 2021. *This is no ordinary spying. Our most intimate selves are now exposed | Arundhati Roy*. [online] Available at: <https://www.theguardian.com/commentisfree/2021/jul/27/spying-pegasus-project-states-arundhati-roy> [Accessed 30 September 2021].

[6] Pib.gov.in. 2021. *IT Minister Shri Ashwini Vaishnaw's Statement in Parliament on "Alleged use of spyware Pegasus to compromise phone data of some persons as reported in Media on 18th July 2021"*. [online] Available at: <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1736803> [Accessed 30 September 2021].

[7] The Information Technology Act,2000 (Act 21 of 2000)

[8] The Indian Telegraph Act,1885 (Act 13 of 18851)

means a research that has been carried out on a legal proposition or preposition by the way of analyzing the existing statutory provision and case by applying the reasoning power[9]. In order to substantiate this paper, I have relied on case studies, compared international provisions and critical analysis. Comparative analysis enabled me to compare various judicial interpretations. The data collected is from books, journals, articles and case studies.

(B) Review of literature

The literature review used for this paper are as follows

"Report of the Group of Experts on Privacy", the planning commission of India, chaired by Former Chief Justice, High Court of Delhi, Justice Ajit Prakash Shah. The report recommends changes to the existing privacy law policy. As per the report, privacy law in India should be based upon the principles of consent, access and correction, security, openness and accountability.

"A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. The report emphasizes the need to devise a legal framework in the growing global digital landscape. According to the committee, in order to safeguard personal data of the citizens, the government must aspire to the common public good of both a free and fair digital economy. The committee recommended that data should be processed for "clear, specific and lawful" purposes only. Personal data should be collected in order to avert the offences. Once the purpose of the data is over, the information should be erased if it is no longer in the public interest.

"Draft International Principles on Communications Surveillance and Human Rights", the Centre for Internet and Society, Elonnai Hickok, the report aims to provide guidelines for communication surveillance for industry, business, human rights groups and government. It highlights thirteen principles. Any limitation to the right to privacy must be as per the law. Surveillance should be limited to those collection which are necessary to achieve a legitimate aim.

II. LEGAL LANDSCAPE

This paper primarily revolves around the question whether the existing legislation regarding surveillance law in India are adequate. For this, I will analyze the two main legislation related to surveillance (1) the Indian Telephone Act, 1885 and (2) the Information Technology Act, 2000. These were introduced as safeguards to curb unauthorized surveillance. The relevant

[9] Dr. S.R. Myneni, "*Legal Research Methodology"* 39 (Allahabad Law Agency, 5th ed. 2012)

 [ISSN 2581-5369]

provision under Indian Telephone Act, 1885, is section 5 of the act. The section allows the central government and state government to issue orders of surveillance for (1) any "public emergency" or in the interest of "public safety" and (b) the interests of the sovereignty and integrity of the country; State security; in order to maintain friendly relations with foreign states; to maintain public order; for preventing incitement to the commission of an offense. The order can only be issued by the Secretary in the Ministry of Home Affairs[10].

Under the Information Technology Act, 2000, section 69 allows the Central Government and the State Governments to issue directions for the monitoring, interception or decryption of any information transmitted, received or stored through a computer resource. Such interception can be conducted to protect the sovereignty or integrity of India; Defense of India; Security of the State; Friendly relations with foreign States; Public order; Preventing incitement to the commission of any cognizable offense relating to the above; and for the investigation of any offense. The Secretary of Home affairs is the competent authority under the act to issue orders of surveillance[11]. The use of surveillance software to spy on individuals is a criminal offence under section 66B of the act. Under section 43 of the IT Act, any person without permission of the owner of a computer, accesses or secures access to the computer system in order to downloads, copies or extracts any data from, introduces or causes to be introduced any computer contaminant or computer virus into, damages, disrupts, or denies access to such computer system or charges services availed of by one person to another person can be made liable to pay compensation to the extent of Rs. 1, 00, 00,000/-.

Surveillance is conducted through Internet Service Providers (ISP) and Telecom Service Providers (TSP). While issuing licenses to the Department of Telecommunications of the Ministry of Communications and Information Technology, mandate a license agreement, under which the ISP's and TSP's have to conduct mass surveillance in order to operate. Unified Access Services (UAS) License Agreement can be applied to both ISPs and TSP's, it is an umbrella license agreement. The Department of Telecommunications has issued several guidelines to intercept communication in cases of public emergency or safety. The license Agreement gives the Government the right to inspect and monitor ISP's. TSP's are required to inform the government of any malicious and obnoxious communication. As per the agreement, the government can even intercept communications through basic telephone services. The government can gain information about the individual calling number, the time, duration and

[10] Rule 419A (1), Indian Telegraph Rules, 1951.
[11] Rule 2(d), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

 [ISSN 2581-5369]

date of interception, the location of the individual, even failed call attempts.

III. INTERNATIONAL SURVEILLANCE PRACTICES

The need for protection of personal data has gained prominence with the shift to online economic and social activities. Large amounts of information are transmitted, stored and collected across the globe. The importance of privacy and data protection is being recognized with the growth of international trade. Most developed countries have adopted a data protection legislature. Despite regional differences, these legislatures have few common core values. Analyzing these set of core values will be a good starting point to draft data protection law which are compatible and harmonized.

Under Art.12 of the Universal Declaration on Human Rights[12] and Art.17 of the International Covenant on Civil and Political Rights[13], a person cannot be subjected to arbitrary interference with his privacy whether at home or in correspondence. It prohibits attacks upon a person's honor and reputation. Every individual has the right to protection against such interference. The European Union in 2018 enacted the General Data Protection Regulation (GDPR)[14] to consolidate and regulate the data protection within the EU. The act encompasses the values enshrined in the Universal Declaration of Human Right and International Covenant on Civil and Political Rights. The GDPR is built around the concept of lawful processing of data. The GDPR endows individuals with great rights over their data. The consent of the data subject should be freely given. The data subject can assess and correct the data. The processing of personal data must always be lawful, fair, and transparent. It must fall under the five categories of lawful processing. The personal data of a person cannot be processed unless a data controller has individual consent. The American approach to data protection is similar to the EU. Protection of personal information is enforced through federal and state laws in fields ranging from health, education, finance, video rentals and consumer protection laws. The data can be collected and processed unless it is forbidden by specific laws. The American policies do not adequately protect against interference and attacks by private and public entities.

[12] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: https://www.refworld.org/docid/3ae6b3712c.html [accessed 7 August 2021]

[13] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.refworld.org/docid/3ae6b3aa0.html [accessed 7 August 2021]

[14] European Union, "REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/ EC (General Data Protection Regulation)

IV. JUDICIAL INTERPRETATION OF SURVEILLANCE AND RIGHT TO PRIVACY

The right to privacy has been upheld by the courts in many cases. In the case of Kharak Singh v. Union of India[15], the court held that the right to personal liberty is not only a right to be free from restrictions placed on movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Further, Govind v. State of M.P[16], the Supreme court recognized right to privacy as a fundamental right and laid down certain exception where reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence[17].

In the case of R. Rajagopal v. Union of India[18], the Supreme Court recognized the right to privacy which protects personal property from unlawful governmental invasion. In this case a prisoner convicted with six-murder, wrote an autobiography from the petitioner's magazine. The respondent, State of Tamil Nadu, Inspector General of Prisons and the Superintendent of Prison, prohibited the prisoner from publishing his autobiography. The Superintendent forced the prisoner to write a letter to the publisher expressing his desire not to publish. The court held that the prisoner had the right to publish his biography. It recognized the right to privacy as a fundamental right but not an absolute right. The court laid down exception to the rule that a person's private information cannot be invaded (1) if he voluntarily invites controversies. (2) If the publication is based on public records. (3) Public officials do not have a right to privacy in acts and duties relevant to the discharge of their official duty.

In the landmark case of People's Union for Civil Liberties (PUCL) v. Union of India[19], a petition was filed by the PUCL against incidents of telephone tapping after a report on "telephone tapping" of politicians was released by the CBI. The petition challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885. As per the report many telephones were intercepted without the permission of the government of India. The files related to interception were not maintained properly. The court laid down the following rules for interception.

[15] AIR 1963 SC 1295
[16] AIR 1975 SC 1378
[17] INDIA CONST.art.19,cl.2
[18] 1995 AIR 264
[19] (1997) 1 SCC 301.

 [ISSN 2581-5369]

1. An order of telephone tapping under section 5(2) of the Indian Telephone act, 1885 should be issued by the Home Secretary, Government of India of the Central Government and Home Secretaries of the State Governments.
2. Interception should be in the course of their transmission by means of a public telecommunication system. The information intercepted should be disclosed.
3. Interception will be considered necessary if there is no other reasonable means to acquire the information.
4. Communication of only those particular persons specified or described in the order or one particular set of premises specified or described in the order can be intercepted.
5. The order under Section 5(2) of the Act will cease to have effect at the end of the period of two months from the date of issue.

In the case of Justice K.S. Puttaswamy(Retd.) and Anr v. Union of India and Others[20], the 9 judge bench of the Supreme Court unanimously upheld that the Constitution of India guarantees to each individual a fundamental right to privacy. The court noted that with the growth of highly sophisticated communication technology the right to golf telephonic conversation in the privacy one's home or office without interference is increasingly susceptible to abuse. The right to privacy imposes on the State a duty to protect the privacy of an individual, corresponding to the liability that is to be incurred by the state for intruding on the right to life and personal liberty. An act of the State violating the right must satisfy the test of the applicable Article apart from the test of being fair, just and reasonable under Article 21.

By interpreting the above cases it is clear that the judicial system has on several instances upheld the right to privacy as a fundamental right. However, this right is not absolute and can be imposed with restriction. Such restriction should be reasonable and imposed through due process[21].

V. PERSONAL DATA PROTECTION BILL, 2019

The current laws recognize the right to privacy as a natural and inherent right, yet there is significant potential for abuse. The procedure to collect, process, disclose, make available or otherwise use personal data for the purpose is not laid down. Changes in privacy are necessary to restrict unauthorized surveillance and access of personal data to third parties. In order to address the problems, the government introduced the Personal Data Protection Bill in 2019[22].

[20] (2019) 1 SCS 1
[21] Maneka Gandhi v. Union of India, (1978) 1 SCC 248
[22] "Personal Data Protection bill, 2019," Pub. L. No. 373 of 2019, accessed August 5, 2021, http://164.100.47.4/

The bill aims to safeguard individual data by creating policies which will regulate the collection and use of data. The proposed bill increases the role of state authority in surveillance. If the bill is enacted it will be applicable to all enterprises in India. This would affect all forms of businesses. The bill also places a huge emphasis on consent. The data will be collected after informing the data principle the purpose of data collection. However, in certain circumstances the necessity of consent and notice can be exempted such as prevention and detection of .unlawful activity. The biggest setbacks with this legislature is the lack of checks and balances for surveillance. The proposed bill does not address the loopholes of the previous legislatures. The bill does not provide a penalty for non-compliance with procedure. The consent given during surveillance will be meaningless. As the consent agreement is complex and incomprehensible, an individual will not have the choice to negotiate his interest. Therefore, it renders the consent clause redundant. Since the proposed bill will have a significant impact on the economy, it is necessary to carefully study its impact.

VI. SUGGESTIONS AND CONCLUSION

Surveillance is an intrusive act which adversely affects the right to freedom and violates the basic construction of our constitution. The existing legal provision are vague and lack accountability. However, with the rise in acts of global terrorism it has become necessary to take precautions against nefarious activities. In these instances, the government has to take intervening steps to avert potential danger. Decisions for mass surveillance should be made by weighing the benefit and harm caused. Such a decision should be made according to the principles of necessity and proportionality. The current laws do not account for surveillance conducted through CCTV cameras and drones. The circumstances where surveillance can be conducted under the policy are very wide and ambiguous. There is an urgent need to review the data protection policy in Indian, in order to stop the infringement of personal data.

In a democratic society, the purpose of any surveillance should be legitimate. Every surveillance activity should meet the standard of procedure provided in the legislative act. There should be transparency about any equipment or facility purchased for surveillance. An independent commission should be established to oversee all authorized surveillance and provide redressal in cases of illegal breach. The data collectors should be required to notify individuals with regards to what personal data is being collected, the purposes and uses for such data collection,. The individual should be informed if such personal data will be disclosed to third parties. They should have the right to access the personal information which is being

BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

 [ISSN 2581-5369]

collected and make corrections or delete data if it is incorrect. The personal information collected should be necessary to the objective. Such personal information should be collected as a last resort, if there is no alternative option of gaining information. Prior notification and consent should be taken from the individual. All surveillance should be fair and through lawful means. The data controller should be accountable for complying with the procedure.

*****

 [ISSN 2581-5369]