ISSN :2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 6

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Quarterly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

The Pegasus Project: Inexhaustible State Surveillance

Authored By- Sthapitha Thangamma

ABSTRACT

Terrorism and environmental catastrophes are escalating as populations become fearful of the contemporary age menace of interception and surveillance. While the Information Technology Act 2000 and the Indian Penal Code1860 respectively have several provisions pertaining to the protection and processing of information, India's traditional laws slow to a crawl that of technological improvements. There is software, legal or illegal, capable of transmitting a target's whereabouts and assisting in mass surveillance of the state in jurisdictions where non-consensual surveillance technology is not authorized under Indian Cyberlaw. International treaties alone are laughably inadequate to rein in domestic security and privacy issues. Furthermore, the supreme law of the land emphasizes the constitutionality of Pegasus software used in India, given Indian Constitutional Articles 19 and 21. The Puttaswamy judgment was unable to comprehend the broader spectrum of Privacy permission. This article aims not to evaluate if the government allegedly acquired Israeli software.

Nevertheless, it is essential and significant to ascertain the extent and liability of the state's powers over its citizens' data and transmission, given that surveillance is administratively permitted given specific procedures are followed. In today's society, it is constructively impossible to comprehend espionage state of the art. What may be done relatively is to enforce restrictions that achieve a balance between the benefits and drawbacks of such evolved forms.

KEYWORDS:*Privacy, Security, Interception, Surveillance, State, Technology*

INTRODUCTION

State Surveillance has become an increasingly worrying subject in the present day. The concept of Privacy established by the Indian Judiciary focuses on the individual ambit. But in reality, the compass is much wider. Article 21 guarantees the Right to Privacy as part of life and liberty, but the Government continues to watch its citizens intensely. They use technology that is readily available and accessible in the market, without disturbances in its design and development; copyrights and licenses are issued quite freely. The Puttaswamy Judgement brought with it specific recommendations to strengthen the privacy regime in India, including the right to be forgotten and data protection authority. Many international case studies and developments show the reality of a threat like state surveillance. For instance, Mason's Model, which is Privacy, accuracy, property, and accessibility (hereinafter referred to as "PAPA"), is an accurate analysis answering the question 'of why' we fear privacy breaches and 'how' we can prevent this from happening. We will discuss these concepts intensely while associating them with the newly acquired spyware, Pegasus, by the Indian Government. Pegasus is a software that maintains a list of people spyed on, commonly known as mass surveillance. The author will discuss the new age threat, which is Privacy and data breach, how institutions in power manage to control extensive data, briefly explain the overview of Indian data and privacy laws while conducting a comparative analysis with US and EU, go through a few case studies, discuss the commonly used defenses and conclude with a preach for sticker and more legitimate privacy security laws in the Indian territory.

Privacy In India: An Underrated Postulation

The desire to have a ‘personal life’ is inherent in every human being, more so, in a world like today where books are open than close. Supporters of privacy have time and again stressed on the bane that is technological developments. Digitalization in India is highly appreciated, considering the literacy and education levels of the population. It has not only made life of the rich easier but facilitates in enhancing lives of the poor. For instance, all farmers and low-income people are entitled to payments via UPI/GOOGLE PAY. Or the unique identification number which made direct cash transfers mandatory, to cook gas subsidy.[1] This prevents their exploitation and corruption by elite sections of society. However, in the name of data collection, there is a directly proportionate increase in cyber crimes, breach of privacy and threat to national security. The Aadhar initiative that came out in 2010 was acceptable as long as data leakage was controlled. It was the first time in India, where a vast populations’ private information had a designated data base.

[1] Pahal Handbook, Ministry of Petroleum and Natural Gas, Government of India, http://petroleum.nic.in/dbt/DBTL_Handbook.pdf. Last accessed on 02.05.2022

On information being shared voluntarily, the same may be said to be in confidence and any breach of confidentiality is a breach of the trust.[2]

This Aadhar issue embodies the privacy breach aspects accompanied by India's AI agenda. Artificial intelligence has been implemented in various spheres, including healthcare, agriculture, education, smart cities, and infrastructure. For instance, using AI in healthcare, it is essential to address challenges related to high barriers to accessing healthcare facilities, particularly in remote locations with poor connections and an insufficient supply of healthcare specialists.[3] Security is intrinsically linked to the origins of liberty, equity, human respect, uniqueness, and everyday significance. While the protection framework is not new, the convention of security as a right is comparatively modern. Subsequently, as social orders undergo significant change, it entails a re-conceptualization of the right to protection. The issue emerges as to how far it should be safeguarded and thefocusofdecisionalprivacyisonfreedomfrominterferencewhenmakingcertainfundamental decisions. In contrast, informational privacy is concerned with the use, transfer, and processing of personal data generated in daily life.

The majority of people fail to acknowledge the stark distinction between cognitive and procedural confidentiality. The objective of decisional privacy is to maintain the potential to make certain essential choices without interference. By distinction, informational privacy refers to the utilization, transmission, and processing of personal data generated daily. For instance, the Aadhar database contains citizens' biometric and other personal information. This is not a conventional collection but rather a relatively close instance of informational privacy. According to the United States' IITF Principles, information privacy is "an individual's concept to govern the circumstances on which personal information, i.e., data that can be used to identify the individual, is accessed, released, and utilized." Furthermore, personal information does not always emphasize sensitive or powerful information. Personal information is essential to the source of the problem since it serves as an identifying trap for an individual in his daily life.

[2]Solove, D., 1991. 10 Reasons Why Privacy Matters. https://www.teachprivacy.com/10-reasons-privacy-matters/. Last accessed on 02.05.2022

[3]*A fundamental Study for Artificial Intelligence and Indian Legal Perspective*, IJAST, 29 (5), 2020. Last accessed on 02.05.2022

The Threat Of Pegasus On Privacy And Life

Citizens need to be protected from unlawful surveillance to protect their fundamental right to privacy. The court has taken a strong stance against surveillance on individuals and said that in a democratic society, spying on individuals cannot be permitted except by following procedure estbalished by law. Unlawful surveillance can have adverse impacts on society and majorly violates the rights of citizens according to the Consitution. Article 21 guarantees right to privacy as part of the fundamental right. Unlawful spying also violates the right to freedom of speech and expression, protected by the Indian Constitution under Article 19(1)(a). This flows from the logic that surveillance can intrude and impact the way in which people think and communicate with their neighbours about their opinions on social and political issues and it restricts the flow of important information in the society because many things get censored or there are chances that citizens don't speak up their minds in fear of getting caught by the state authorities. Supreme Court bench cited a quote from George Orwell's 1984 novel "If you want to keep a secret hide it from yourself." Reference of this quote is very insulting for any state and working of its government; the book written in 1984 is about a state where everyone is suppressed and it revolves around the theme of government surveillance and dictatorship.

The software through something called a 'rogue cell tower' pretends to be a legitimate cellular company and compels mobile phones anywehere near it to connect to it. Once this connection is established, the attacker can easily become a part of the intercepted traffic. Let us first understand that Pegasus is not 'bad' or to be viewed as a 'negative'. It is only a legal product of an organisation, utilised for unlawful objects within the country. It is able to achieve this by "zero click installations", that is, without requiring interaction by the target.[4]

The Pegasus Project revelations raised two important questions, the integrity and sustainability of democracy and the future of press freedom in India. Journalists who have been targeted by Pegasus include a number of notable names, some of whom have investigated and covered up allegations of corruption in a defense acquisition. Several senior journalists have appealed to the Supreme Court of India, alleging that the targeted surveillance is a "disproportionate invasion of privacy". Puttaswamy points out that there is a fundamental right to privacy according to Article 21and after the 44th Amendment to the Constitution of India, the government cannot violate this provision even after declaring a state of emergency. The Indian Legislative System currently holds no law specifically remedying privacy violations and preventing surveillance. It merely acts as a disputable shield and not a sword. There is no law that prescribes explicitly remedies for privacy violations at the statutory level, and the Supreme Court's decision in Puttaswamy is an

[4]https://indianexpress.com/article/explained/pegasus-whatsapp-spyware-israel-india-7410890/. Last accessed on 02.05.2022

unproven shield against privacy violations rather than a sword. The Personal Data Protection Bill, which aims to codify certain aspects of privacy and provide a minimum level of protection against violations of this right, has been approved by the committeesof parliament delayed since 2019. Currently, the legal framework governing India's surveillance activities has many loopholes. The main problems are the concentration of power with the executive branch and the lack of independent judicial control. Specifically, requests for oversight, both at the federal and state levels, are issued by a senior official in the Department of the Interior. In addition, the current supervisory regime does not provide for an effective judicial remedy independent of executive power. Finally, the targeted use of surveillance must be carried out in accordance with the principles of legality, necessity, and proportion as recognized by the Supreme Court of India and as set forth in international human rights law.

According to NSO Group, the Pegasus spyware collects data on specific suspected criminals and terrorists. Its use to target civil society, journalists, lawyers, and others, disclosed through Project Pegasus, represents a clear violation of international human rights law. Based on the Universal Declaration of Human Rights (Article 12)[5] and the International Covenant on Civil and Political Rights (Article 17)[6], international human rights law establishes a right to privacy. However, it is a right to privacy but cannot be arbitrarily compromised. Or illegal manner. Interestingly, while ratifying the ICCPR, India did not reserve article 17. Violations of this right are particularly dangerous because they affect many other rights, such as freedom of speech, freedom of association, and freedom of association and other rights, including the right to life.

The Use Of Technology On Inspection Of Citizens: Adequate Legislations?

Surveillance by nature is an activity undertaken without the knowledge of the person being inspected. This implies the necessity for strict legislation that elaborates on the scope of surveillance in nature, based on justifications. In India, there are primarily two laws that deal with surveillance; the Telegraph Act of 1885 and the Information Technology Act 2000. Section 5(2) of the Telegraph Act permits the government to intercept calls in situations of necessity as deemed fit by them- security of state or welfareofthe public. It also clearly specifies that interception cannot be made against country journalists, even if the law considers interception lawful.

[5] Universal Declaration of Human Rights, Art.12
[6] International Covenant on Civil and Political Rights, Art.17

In 1996, the Supreme Court interfered in the amalgamation of privacy, rights, and surveillance matters in

Public Union for Civil Liberties v. Union of India[7]. In this case, the court held that the Telegraph act has no provisions focusing on the larger ambit of surveillance and is very ambiguous. It, therefore, set out guidelines to be mandatorily followed whileinterception takes place by the government. The interest of the Supreme Court was drawn when the CBI was accused of tapping the phones of politicians. “Tapping is a serious invasion of an individual’s privacy. With the growth of highly sophisticated communication technology, the right to sell telephone conversations in the privacy of one’s home or office without interference is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of Subrosa operation as a part of its intelligence outfit, but at the same time, citizen’s right to privacy has to be protected from being abused by the authorities of the day.”[8]

Another statute that parodies less explicitly concerning surveillance is the information technology rules of 2009. All electronic data communications are interceptable within information technology law. Governments must rely on IT and telecom regulations toexploit spyware such as Pegasus legitimately. In accordance with the restrictions specified in Section 5(2) of the Telegraph Law, Article 19(2) of the Constitution of India and Section 69 of the Information Technology Act broadens the concept of interception, surveillance, and digitally decoding; information "to investigate a crime." In 2012, the Planning Committee and the Expert Committee on Privacy Affairs were entrusted with discovering loopholes in the law concerning privacy rights, presided by former Chief Justice AP Shah of the Delhi High Court. Concerning surveillance, the committee stated that legislation varies according to permits, "interception type," "granularity of information that can be intercepted," level of expertise from service providers, and "delete and store" censored data.

[7] 1996 Supp 10 SCR 321

[8] **Apurva Vishwanath, Explained: The laws for surveillance in India, and concerns over privacy, August 3, 2021https://indianexpress.com/article/explained/project-pegasus-the-laws-for-surveillance-in-india-and-the-concerns-over-privacy-7417714/. Last accessed on 02.04.2022**

CONCLUSION

Today's technological advancements are not only essential but also irrational. The essential advantage for developers of this type of software is our emphasis on it. We are constantly on the lookout for cutting-edge software and technology, including applications and social networking sites[9]. Nevertheless, we must be vigilant of the internal espionage that may be embedded in these devices, which may pose a threat to our personal safety. Due to a lack of compliance, perpetrators, including government officials themselves, benefit from security vulnerabilities. This country's trajectory illustrates the dire necessity for comprehensive enforcement of monitoring legislation. Without it, the lives of Indian nationals could be jeopardized both at an international and national level.

Bibliography

- Information Warfare Monitor. Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, March 29, 2009. http://www.nartv.org/mirror/ghostnet.pdf.
- Information Warfare Monitor and Shadowserver Foundation. Shadows in the Cloud: Investigating Cyber Espionage 2.0. Information Warfare Monitor and Shadowserver Foundation, April 6, 2010. https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf. Kaye, David.
- Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Human Rights Council, June 2019. https://citizenlab.ca/wp-content/uploads/2019/06/Special-Rapporteur-report-Surveillance-an d-human-rights.pdf.
- Kazansky, Becky. Digital Security in Context: Learning how human rights defenders adopt digital security practices. Tactical Technology Collective, 2015. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf
- Sinha, M., Majra, H., Hutchins, J. and Saxena, R., 2018. Mobile payments in India: the privacy factor. International Journal of Bank Marketing.
- Chatterjee, S., Kar, A.K. and Gupta, M.P., 2018. Alignment of IT authority and citizens of proposed smart cities in India: System security and privacy perspective. Global Journal of Flexible Systems Management, 19(1), pp.95-107.

[9] Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune. Hacking Team's US Nexus. Citizen Lab, February 28, 2014. https://citizenlab.org/2014/02/hacking-teams-us-nexus/. Last accessed on 02.05.2022