INDIA'S DIGITAL PANOPTICON: INTERCEPTION, SURVEILLANCE, AND PRIVACY

Akshat Shrivastava, B.B.A. LL.B. (Hons.), Babasaheb Bhimrao Ambedkar University, Lucknow

ABSTRACT

The Panopticon was designed by Bentham as a structure where the guards can watch the prisoners constantly without the prisoners knowing when they are being watched. While the original Panopticon was a physical structure, the modern world has witnessed its evolution into a digital Panopticon that is far more pervasive and potent. This article explores some of the surveillance tools that make up India's modern day digital panopticon. The article explores the use of spyware, central monitoring system, and facial recognition technology for surveillance of citizens. The article further explores the legal aspects in relation to such surveillance methods including the lack of proper oversight and privacy issues. It critically analyzes how these surveillance methods, owing to the absence of strict privacy laws in India, present a potential threat to individual rights, civil liberties, dissent, and democratic values. The article then concludes with highlighting some suggested improvement.

Keywords: Surveillance, Interception, Privacy, Panopticon, Section 5(2), Telegraph Act, Section 69, IT Act, Central Monitoring System, Facial Recognition Technology, KS Puttaswamy

Introduction

The Panopticon, originally proposed by Jeremy Bentham in 1791 as a prison design that enabled the constant surveillance of the prison inmates by prison guards without the inmates knowing when they are being watched, finds its sinister reincarnation in the modern-day digital regimes in the form of digital surveillance. Unlike Bentham's physical tower, the digital panopticon operates through encrypted intrusions into smartphones, scrutiny of online activities, and biometric databases that render privacy a precarious illusion, with citizens as prison inmates and the government as the surveilling prison guard of the panopticon. What aggravates the situation is that unlike Bentham's stationary guards, the modern-day surveillance software like Pegasus can turn our phones into pocket-sized panoptic towers, not only monitoring our every activity and movement but also influencing us psychologically, without us being able to notice it.

In India, the power to surveille has been granted to the State by opaque laws that lack proper procedural safeguards against the inappropriate exercise of such power. Section 5(2) of the Indian Telegraph Act, 1885 and Section 69 of the IT Act, 2000 allow the government to intercept communications, digital activities, and information stored in a person's computer in specific conditions and under certain rules. These rules and procedures, however, are not transparent and offer very weak protection to the surveilled. Furthermore, the recent allegations comprising the use of Pegasus spyware on ministers, opposition leaders, journalists, activists, judges, religious leaders, administrators and political strategists have intensified concerns over unchecked state surveillance, raising serious concerns regarding privacy violations, human rights, freedom of speech, and democratic accountability. This puts the dissenting voices into an uncertainty – whether they are being surveilled.

"The perfection of power tends to render its actual exercise unnecessary". The knowledge that you may be under constant surveillance, even when the surveillance is discontinuous or absent, is enough for the citizens to self-regulate themselves, becoming docile bodies that conform to the societal norms, so as to not be punished for their violations. This psychological tyranny of the panopticon – where uncertainty breeds self-censorship – is amplified in the digital realm. Activists, protestors, journalists, and politicians, who seek to criticize the actions of the state, fear surveillance of their private and sensitive information. As a result, they dilute their critiques and muzzle their dissenting voices.

The Supreme Court of India in K.S. Puttaswamy vs. Union of India (AIR 2017 SC 4161) has recognized the Right to Privacy as intrinsic under Article 21 of the Constitution of India. Further, privacy is the key to freedom of thought and expressions. A person has a right to think and has the freedom to choose the person he wants to share or express his thoughts to. This makes the Right to Privacy intrinsic in the freedom of speech and expressions under Article 19(1)(a) of the Constitution. The right to travel freely within the territory of India (Article 19(1)(d)), the right to travel abroad (Article 21), the right to choose the nature of work (Article 19(1)(g)) are all part of a person's private decision making and may be associated with the right to privacy depending upon the situation. The scope of right to privacy, thus, is not limited to single right or article.

Surveillance by the government through spyware, use of facial recognition cameras, and Aadharbased dataveillance not only infringes upon the privacy of the citizens but also deprives them of a dignified life under Article 21, equality under Article 14, and chills their right to free speech, expression, movement and dissent under Article 19 of the Constitution. The lack of transparency in the surveillance process, accountability of the surveilling agency, and procedural safeguards with the surveilled further worsens the situation for the citizens by violating the principles of natural justice.

This scope of arbitrariness in the government's action must be tackled with in order to avoid moving towards eventually becoming something more serious than Foucault's disciplinary society, an Orwellian disciplinary society. India's embrace of mass surveillance methods and facial recognition systems combined with lack of accountability and transparency risks institutionalizing Orwell's nightmare: a society where surveillance is omnipresent and dissent is erased.

Anatomy of Digital Surveillance

Surveillance may be defined as the scrutiny or systematic observation of individuals, groups, and situations through the application of technical means to gather or generate information.[1] Early surveillance comprised spy networks, informants, and record keeping systems used by rulers to monitor populations and gather intelligence. Modern surveillance, on the other hand,

[1] *Marx, G.T., Surveillance studies, 2 INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 23, 735 (2015)*

encompasses a wide range of digital methods including spyware, biometric surveillance, satellite surveillance, communication interception, License Plate Recognition, social media surveillance, location tracking, AI and big data surveillance that do not even require a physical person to keep an eye on someone.

In India, surveillance is conducted through various agencies and systems including the Central Monitoring System, Network Traffic Analysis System, National Intelligence Grid, and Facial

Recognition Technology. The Indian police in several places `have been recently regularizing Facial Recognition Technology (FRT) through facial recognition cameras and drones. The Central Monitoring System (CMS) is used to intercept and monitor communications including voice calls and messages. Smart city projects contribute to mass surveillance by installing CCTV networks with AI-driven analytics. The Aadhar card IDs are linked with the individual's phone numbers, bank accounts, and pensions other than holding other essential information including biometrics. The National Intelligence Grid (NATGRID) integrates databases from various agencies allowing real-times access to information on an individual's financial transactions, communication records, passport data, vehicle registration details, and other personal information.

There have been drastic developments made in the digital surveillance technology in the recent years with advanced techniques being used for monitoring individuals with great accuracy. However, the emergence of such sophisticated surveillance methods intensifies risks relating to privacy, individual freedoms, dignity, and data security. Furthermore, such expansion of surveillance capabilities heightens the risk of abuse, overreach, and unchecked controls if it lacks proper oversight. Such are the risks in cases of the use of spyware, intercepting surveillance methods, facial recognition system, and Aadhar based dataveillance by the government.

The Pegasus Spyware

It was confirmed by Amnesty International's Security Lab, after its forensic investigation, that the phones of Anand Mangnale and Siddharth Varadarajan, Investigative journalist of the OCCRP and Founding Editor of The Wire respectively, had been targeted and attacked by the

Pegasus Spyware.[2] This followed a disclosure that the devices of some Indians users, among other users, were affected by a vulnerability identified by WhatsApp in its software that enabled spyware infiltration by Pegasus in their devices which was acknowledge by the then Minister of Law and Electronics and Information Technology in a statement made in the Parliament on Nov 20, 2019. An investigation under the Pegasus Project initiative conducted by 17 journalistic organizations based on some 50,000 leaked numbers which were allegedly under surveillance by clients of the NSO Group through the Pegasus software discovered that nearly 300 of these numbers belonged to Indians, many of whom were political leaders, journalists, and members of the judiciary. These reports increase serious concerns regarding infringement of citizens' privacy and freedom by the Indian government.

A petition has been filed in the Supreme Court of India following these incidents where the court has constituted a three members committee comprising experts in cyber security, digital forensics, and networks and hardware to investigate and determine whether the Pegasus spyware was used on the devices of the citizens of India to intercept information, whether any spyware was acquired by the government to be used against citizens, and other related matters.[3]

What Information could it collect

The Pegasus spyware collects information by infiltrating the smartphones of the targeted individuals through methods such as "zero click exploits" and "network injection" where the targeted persons are not even required to click on any malicious link for the virus to enter their phones.[4] It can gather far-more information than conventional surveillance method of wiretapping or telephone interception such as accessing emails, social media communications, call logs, and messages on encrypted applications such as WhatsApp or Telegram. It can also ascertain a user's location, movement status, and direction, in addition to extracting contacts, usernames, passwords, notes, documents, photographs, videos, and sound recordings.[5] Advanced spyware have the capability to activate microphones and cameras without triggering any visible indicators. In essence, any function that a user can perform on their device can be

[2] *Amnesty International Security Lab, Forensic appendix: Pegasus zero-click exploit threatens journalists in India, AMNESTY INTERNATIONAL (Dec. 4, 2023)*

[3] *Manohar Lal Sharma vs. Union of India, 2021 INSC 682*

[4] *OCCRP, How does Pegasus work, Organized Crime and Corruption Reporting Project, ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT (July 18, 2021)*

[5] *Craig Timberg, et. al., Drew Harwell, Q&A: A guide to 'spyware', THE WASHINGTON POST (July 18, 2021)*

similarly accessed by operators of sophisticated spyware. Some variants can even deliver files to devices without user knowledge or authorization.[6]

Self-censorship due to fear of surveillance

Incidents such as the alleged targeted surveillance of journalists, activists, judges, and opposition politicians create an uncertainty that one may be under surveillance at any time. The uncertainty is fueled not only by the alleged incidents but its combination with the lack of procedural safeguards available if the incidents alleged are true, the lack of oversight on the surveillance processes, and the absence of proper laws regulating surveillance activities by the governments. This mere possibility that one is being surveilled compels individuals to self-regulate. It creates fear in the minds of the dissenting individuals ultimately imposing a chilling effect on their freedom to explore, share, and engage with unconventional, controversial, dissenting, or provocative ideas. In simple words, the absence of a firm law to stop the government from surveilling them, even if the actual surveillance is absent, could cause uncertainty and be a medium to prevent the journalists or activists from revealing any information that is against the ruling party such as revelations of corruption by politicians.

Central Monitoring System

The Central Monitoring System (CMS) was first announced by the Government in 2009 following the 2008 Mumbai terrorist attacks. It is a mass surveillance programme of the Indian Government that automated the then existing manual interception and monitoring process through electronic links.[7] The existing system took a very long time and had vulnerabilities in relation to maintenance of secrecy due to manual intervention which was not the case with CMS.[8]

Under the CMS, the Telephone Service Providers (TSPs) are required to integrate their Lawful Interception Systems (LIS) with Regional Monitoring Centres (RMCs) through Interception Store & Forward (ISF) servers.[9] The RMCs are further connected to the CMS. Thus, the data

---

[6] *Id.*

[7] *Press Information Bureau, Government of India, Ministry of Communication, Centralised System to Monitor Communicaitons (27 November 2009), https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=54679*

[8] *Id.*

[9] *Govt. of India, Ministry of Communications and IT, Department of Telecommunications, Amendment 2 of 2013, 800-12/2013-AS.II (11 October 2013), https://dot.gov.in/sites/default/files/DOC231013.pdf?download=1*

intercepted by the TSPs were now automatically transmitted to the RMCs and then the CMS without the need of notifying the nodal officers earlier appointed for the purpose of "lawful interception".[10]

Facial Recognition Technology (FRT)

Facial Recognition Technology (FRT) is a data-driven biometric technology that uses artificial intelligence and machine learning to identify or differentiate individuals based on their facial features. It primarily seeks to accomplish three functions – facial detection, feature extraction, and facial recognition.[11]

The Tamil Nadu police use the Facial Recognition System (FRS) and the Facetagr application to identify criminals and get their data by scanning their face or photograph. The Trinetra application with the help of its huge database of criminals helps UP police to identify a criminal through his face, photograph, name, or past FIRs to get information related to him. The Punjab Artificial Intelligence System (PAIS) is a technology being used by the Punjab police for facial recognition of criminals and suspects. Similarly, many states in India are using Facial Recognition or biometric Technology such as AFRS in Delhi, TSCOP and CCTNS in Telangana, and AMBIS in Maharashtra. The National Crimes Records Bureau (NCRB) has requested for proposals inviting bids of a National Automated Facial Recognition System (AFRS) as a national level project.[12]

Legal Issues

Interception and surveillance are mainly governed in India by Section 5(2) of the Telegraph Act, 1885 read with Rule 419A of the Telegraph Rules, 1951 and Section 69 of the Information Technology Act, 2000 read with IT Rules, 2009. The existing legal architecture is riddled with inadequate safeguards, is inadequate to effectively and efficiently govern surveillance, and is easily bypassed by the government. Further, the government continues to introduce new

[10] *Maria Xynou, India's Central Monitoring System (CMS): Something to worry about?, THE CENTRE FOR INTERNET & SOCIETY*
[11] *NITI Aayog, Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology (2022)*
[12] *National Crimes Records Bureau, Request for Proposal: National Automated Facial Recognition System, MINISTRY OF HOME AFFAIRS, GOVERNMENT OF INDIA (2019)*

surveillance mechanisms that, at times, exceed lawful boundaries, thereby posing a risk to the fundamental rights and civil liberties of individuals. This gives rise to several legal issues.

The Lack of Oversight under Section 69, IT Act

The procedure and safeguards with regards to interception, monitoring, and decryption under Section 69(1) of the IT Act is governed by the IT Rules, 2009[13] made under Section 69(2) of the IT Act. Rule 3 of the IT Rules[14] states that the interception, monitoring, or decryption of information could be carried out only on the written directions of the competent authority, which is, the Union Home Secretary[15], or in the State Government, the secretary in charge of Home Department.[16] The direction may be issued by Joint Secretary of the Government of India duly authorized by the competent authority in unavoidable circumstances.[17] The only safeguard against these orders of interception, monitoring, or decryption is under Rule 22 of the IT Rules that they are scrutinized by a review committee, constituted under Rule 419 of the Indian Telegraph Rules, 1951[18], consisting entirely of executive members i.e., Cabinet Secretary and Secretary in the Departments of Legal Affairs and Telecommunications.

The safeguard against the orders of surveillance, thus, completely lacks judicial oversight. The orders of the executive, in simple terms, is reviewed by the executive itself. As the Principles of Natural Justice apply on administrative processes as well[19], the principle of "Nemo judex in causa Sua" (no one should be a judge in one's own cause) is violated here as the review of the order of the executive body is being done by the executive body itself. This is against the principle of just, fair, and reasonable law enunciated by this Hon'ble court in Maneka Gandhi vs. Union of India[20], thereby violating Article 21 of the Constitution. Limitations on privacy must adhere to due process of law.[21]

---

[13] *Ministry of Electronics and Information Technology, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009*
[14] Id., Rule 3
[15] *Some points on Lawful interception or monitoring or decryption of information through computer resource, PRESS INFORMATION BUREAU (2018), available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556945*
[16] Id.; See also, New Rules for Lawful Interception of Telecommunications, KHAITAN & CO.
[17] *Ministry of Electronics and Information Technology, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3*
[18] *The Indian Telegraph Rules, 1951*
[19] *Uma Nath Pandey vs. State of U.P., AIR 2009 SUPREME COURT 2375*
[20] *Maneka Gandhi vs. Union of India, 1978 SCR (2) 621*
[21] *People's Union of Civil Liberties vs. Union Of India, (1997) 1 SCC 301*

The Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna[22] shows that the Review Committee has to review around 15,000 to 18,000 in every meeting and the meeting is conducted once in two months. Thus, it is practically impossible for the committee to review every order of interception passed by the authorities which indicates of the inefficient and impractical system of checks and balances in the laws relating to surveillance.

CMS and Section 5(2) of the Telegraph Act

The CMS is implemented by the Government as a means of interception under Section 5(2) of the Telegraph Act, 1885 read with Rule 419(A) of the Telegraph Rules, 1951.[23] Section 5(2), in cases such as of public emergency or public safety, allows the disclosure to government or interception of any message or class of message to or from any person or class of persons, or relating to any particular subject if the government is satisfied that it is expedient to do so 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.

Thus, the provision allows for 'targeted surveillance' of messages by persons or messages related to a particular subject that the government deems necessary to be intercepted for national security, maintenance of public order, etc. in times of "public emergency" or in interest of "public safety". CMS, however, is a tool capable of 'mass surveillance'. Further, considering that the Unified License Agreement[24] requires the service providers are required to have the capacity for provisioning at least 3000 numbers for monitoring, it is likely that mass surveillance is undertaken by the CMS.[25] Given these facts, along with the ambiguity over whether interceptions are conducted due to a public emergency or in the interest of public safety, it remains uncertain whether the very nature of the CMS falls within the scope of Section 5(2) of the Indian Telegraph Act, 1885.

---

[22] Srikrishna, B.N., et. al., C.O.E, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, at 125 (2018)

[23] Brief Material for Hon'ble MOC & IT Press Briefing on 16.07.2013, https://cis-india.org/internetgovernance/blog/new-cms-doc-2

[24] Govt. of India, Ministry of Communications & IT, Department of Telecommunications, Licence Agreement for Unified License (Access Services), at cl. 41.16, https://dot.gov.in/sites/default/files/DOC270613-013.pdf

[25] Maria Xynou, India's Central Monitoring System (CMS): Something to worry about?, THE CENTRE FOR INTERNET & SOCIETY

Privacy and Facial Recognition Technology

Some of the biggest concerns revolving around Facial Recognition Technology are regarding data storage and misuse, function creep, privacy infringement, and chilling effect on freedom of speech and expression. The Delhi Police initially acquired Facial Recognition Technology (FRT) to track and identify missing children which was authorized by the direction of the Delhi High Court in Sadhan Haldar vs. NCT of Delhi[26]. However, it was later stated by the Delhi police in an RTI response that the technology was also being used for police investigation.[27] It was reported that the Delhi police has been using the FRT on protestors during the anti-CAA protests and the farmers' protest which is an instance of function creep.

Another problem is regarding the storage and misuse of such data. Although facial data is easy to collect, its storage requires high security standards due to its sensitivity. A breach could result into identity theft, harassment, or extortion. Breached data could be used by hackers to access person's personal information such as social media profiles. The data could also be misused by the authorities themselves. A document signed by representatives of Huawei, a Chinese multinational corporation and technology company, showed that it worked on a camera system which can estimate a person's age, sex, and ethnicity through facial recognition.[28] The report further said that on detecting the faces of the persons of a particular community, it could trigger an "Uighur alarm" – potentially flagging them for police in China.[29]

Further, FRT is capable of causing a chilling effect on the freedom of speech and expression. Facial surveillance in cases of public demonstration and protests muzzles dissent as it could be used to recognize and take action against the persons criticizing the government. "The perfection of power tends to render its actual exercise unnecessary." The fact that the FRT has the capable of exposing the identity of the protestors to the government and police authorities is enough to muzzle their dissent and regulate their behaviour. As dissent is not only a fundamental right[30] but an important aspect of democracy, muzzling dissent threatens

[26] *Sadhan Haldar vs. NCT of Delhi, W.P.(CRL) 1560/2017*

[27] *Anushka Jain, Explained: Delhi Police's Use of Facial Recognition Technology, The Hindu (Aug. 21, 2022)*

[28] *Harwell, D., et. al., Eva Dou, Huawei tested AI software that could recognize Uighur minorities and alert police, report says, THE WASHINGTON POST (December 8, 2020),* https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighurminorities-alert-police-report-says/

[29] *Id.*

[30] *Javed Ahmad Hajam vs. State of Maharashtra, [2024] 3 S.C.R. 317*

democracy.

Conclusion and Suggestions

Far exceeding Bentham's architectural panopticon, the digital panopticon comprising spyware, CMS, and FRT leverage ubiquitous connectivity and powerful algorithms to enable constant and invisible scrutiny reshaping the relationship between state and the citizens. The consequences include erosion of Fundamental Rights under Articles 21, 19, and 14. Potential dissenters become "docile bodies" due to the knowledge of being surveilled. Further, there is always a scope of function creep, misuse, and institutional arbitrariness.

There is a need for a privacy legislation that enshrines necessity, proportionality, transparency, and accountability in matters of surveillance. The legislation must establish clear limits of the use of Central Monitoring System to prevent mass surveillance not authorized by the law. There must be a judicial pre-authorization over matters of surveillance and judicial oversight over the orders of interception, monitoring, or decryption rather than the current executive oversight that undermines the principles of natural justice. The involvement of judicial oversight would eliminate arbitrariness.

When activists fear encrypted calls, journalists dilute critiques, and judges avoid controversial rulings, democracy itself becomes a casualty. Without urgent reforms, India risks normalizing a reality where the digital panopticon replaces constitutional governance.