VOL.4 ISSUE 1

DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY

ISSN: 2456-7280

THREAT OF SURVEILLANCE OF CITIZENS' DATA WITH RESPECT TO SECTION 69, INFORMATION TECHNOLOGY ACT, 2000

-Pragya Srivastava[1]

ABSTRACT

In India, we have a peculiar blend of enormous volumes of transparency of data and very small accountability when it comes to the question of the extent of surveillance of individual/mass data and intelligence agencies. Present laws and licenses in India that permit such surveillance involve a substantial possibility of misuse since the country is devoid of enough privacy protections. A privacy law is considered essential to make sure that data is not held indefinitely, it not shared without the knowledge of the owner or is revealed to unauthorized third parties and that such parties can not have any access to the data accumulated and intercepted. In a democratic administration like ours, surveillance should be agreed upon only under a legal permit but due to the absence of any such explicitly effective legislation deprive the subjects of the state from their basic right to privacy.

Despite this progressive view of the country and pending bills regarding right to privacy, the Ministry of Home Affairs (MHA) in an order dated 20-12-2018 provided the explicit power of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer to 10 Central Agencies in an arbitrary move.

This order was given in exercise of the powers under Section 69 (1) of the IT Act, 2000 read with Rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which says: "The competent authority may authorise an agency of the government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of Section 69 of the Act (the Information Technology Act, 2000)."

All of the above information states that "not just calls or emails, but any data found on a computer can be intercepted. The agencies will also have powers to seize the devices."

[1] Student, Faculty of Law, University of Allahabad, Prayagraj

The current note would analyse the repercussions caused by such notification and its effect on every individual consumer of the digital services and Indian democracy.

Introduction

It has become appallingly obvious that our technology has exceeded our humanity – Albert Einstein

The Ministry of Home Affairs (MHA) in an order[2] provided the power of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer to 10 Central Agencies. This has restarted an old conflict between government policies focusing on surveillance and the individual rights of the citizens.

The notification authorises the following agencies for such interception and decryption of data on computers of consumers of digital communications.

1.Intelligence Bureau

2. Narcotics Control Bureau

3.Enforcement Directorate

4.Central Board of Direct Taxes

5.Directorate of Revenue Intelligence

6.Central Bureau of Investigation

7.National Investigation Agency

8.Research and Analysis Wing

9.the Directorate of Signal Intelligence

10.The Delhi police commissioner

This section wasdeveloped from the Indian Telegraph Act, 1885, which spoke of the objective of surveillance as provided in Section 5 emboldening the Central and State Governments of India to continue with the interception of messages, data or information exchange under two non-negotiable circumstances:

(1) in case of any "public emergency" or for the sake of "public safety", and

(2) if it is considered necessary or expedient to do so,

Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a

[2] The Gazette of India: Extraordinary [Part Ii—Sec. 3(Ii)] Ministry Of Home Affairs (Cyber And Information Security Division) Order, 20th Dec, 2018, S.O. 6227(E)

reasonable person[3]. In 2007, Rule 419A had been added to the Indian Telegraph Rules, 1951 providing that generally the orders on the interception of communications should only be issued by the Secretary in the Ministry of Home Affairs. However, it was added in 2008 amendment for safety of the state although the basic object of the Act was to promote e-commerce and provisions like Section 66A and 69A were never meant to be a part of the original act[4].

The section has always been in the controversies as it is loosely formed and has made room for relaxed legislations which can easily turn oppressive. Some of the issues raised against the applicability of the legislation are discussed here.

No review by legislature or judiciary poses a threat to democracy

According to the authorization orders issued by MHA under Section 69(1) the actions taken by the authority must essentially be reasoned in writing, and should be subjected to the procedure laid down in the Information Technology Rules which makes it mandatory for all such orders to be scrutinised by a review committee of the Centre, or the state in question[5] . All review committees set up under this rule comprise of government secretaries meaning thereby that the executives sit in the judgment over its own decisions moving against one of the most basic rule of law contending that no person shall be the judge of their own case. On page 125 of its final report the government-appointed Justice Srikrishna Committee[6] of Experts, which has been given the mission of setting up India's data protection law, cited an urgent need to revise our surveillance laws and recorded, "Executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both".

Pressure of self-incrimation

India believes in a guarantee against testimonial compulsion[7]It had been noted that every positive volitional act which furnished evidence is a testimony[8]. The European Court of Human Rights decision[9] noted that the evidence must have an existence

[3] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[4]Common Cause (A regd. Society) and Anr. v Union of India *(Writ Petition (Civil) 21 / 2013)*
[5]The Indian Telegraph Rules, Rule 419A 1951
[6]https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf , 28. Mar.2019
[7] Indian Const. Art.20, cl. 3
[8]M.P. Sharma v. Satish Chandra, [1954] SCR 1077, pg. 87-88.
[9] Funke v. France, [1993] 1 CMLR 897 25

independent of the will of the suspect. It must be remembered that a password or encryption key has an existence which depends upon the will of the accused, due to its intangibility if the owner of the data refuses to or is unable to disclose it – the password or data has no existence anymore.

However, the Court recognized two main premises for defining 'testimonial compulsion', statements conveying the personal knowledge of a person in respect of pertinent facts that sums up the `personal testimony' thereby coming within the exclusion considered by Article 20(3). In general scenario, such `personal testimony' can be easily differentiated from physical and tangible evidences such as unique body identifiers like DNA, fingerprints or footprints and other such things. Other than this, the concept is that in a number of cases, testimonials can be trusted upon but only for reaffirmation or assessment with facts, trails and evidences in the possession of the investigators beforehand. Hence, even if the password cannot be said to be a testimonial key, the very action of revealing it is equivalent to the personal knowledge of the suspect, which can be different from the independently standing material and tangible objects of facts used for that of comparison and identification. It had been recognized by the American Supreme Court[10] as well.

Additionally, Sec. 69(2) mandates the revelation of information by the accused, which might easily include incriminatory evidence. In this regard, I believe that the testimonial evidence in question is two-fold: First, the information itself being revealed by the accused could have a "tendency of incriminating the accused" or disclose a "guilt character"[11] , the Court noted that the entire question for extending the right presented by Article 20(3) is whether the facts and evidences are capable enough for incrimination by themselves or simply establish a link in the chain of different evidences collected over investigation which could lead to the incrimination in question. In this context, revelation of the subject matter of a data resource by the accused could include incriminatory evidence and in case of refusal by the accused the notification provides for punishment. The fact that at the time of disclosure, the authorities are not aware of whether the information will be inculpatory or

[10]Armando Schmerber v. California, 384 US 757 (1966)
[11]The State Of Bombay vs Kathi Kalu Oghad And Others 1961AIR 1808, pg 128

exculpatory is irrelevant[12] for such accusation. Hence, given the personal and voluntary nature of digital information, the threat of self-incrimination and aid of investigative establishments must be re-considered wholly, instead of blindly following the colonial strategies towards these developments.

Violation of the fundamental Rights: article 19 (1)(g), article 14, right to Privacy

The provision not only encroaches the author's right to speech and expression but also takes the right to data of users under Article 19(1)(a), when access to one's own cyber space is denied. Further, Section 69A bestows unchanneled powers on the union Government which disrupts Article 14.

There is wide-ranging diversion from the principles of natural justice as the blocking directions follow immediately upon the subjective satisfaction of the officer without any notice or advertence to the author/uploader of the content.

As far as the restrictions imposed under section 69A, Sankarnarayan submitted that the provision merely reproduces the grounds listed under Article 19(2). While rational restrictions under Article 19(2) are the basis of qualifying law that restricts free speech, the same cannot likewise be a constraint for determining the grounds for hindering without some objective parameters or guiding principles that clarify precisely the scope of security of the state, public order, friendly relations with states etc[13].

Section 69 can be accused of being violative of Article 14 of the Constitution of India since it gives far-reaching power to the executive and is unreasonable as there is no nexus as to validate having power of such wide scale due to the addition of the which would result in impinging upon constitutional protected rights of person with impunity

India, being a signatory to the Universal Declaration on Human Rights (Article 12) and that of International Convention on Civil and Political Rights (Article 17) has always been obligated to protect the right to privacy as one of the most sacred of fundamental rights. Though the idea of a right to privacy was recognised as a constitutional principle for the first time by the Hon'ble Supreme Court in 1962[14], it

[12]Smt. Selvi v. State of Karnataka, Criminal Appeal 1267 of; 2004 2010(7) SCC 263
[13]Anoop M.K. vs Union of India and Ors**.** *(Writ Petition (Criminal) 196/ 2014)*
[14]Kharak Singh v. State of U.P., AIR 1963 SC 1295.

has been consistently underlined and endorsed in various other cases[15],[16],[17] where it is understood as an entrenched constitutional right under Indian law. Such surveillance threatens individual privacy and must be subject to adequate safeguards. Privacy is a fundamental right guaranteed by the Constitution of India, like all other fundamental rights, the right to privacy is not an absolute right, and can be constrained. However, these restrictions must be: (1) backed by law, (2) for a legitimate state aim, and (3) proportionate.

Thus, any government directive under Section 69(1) of the Information Technology Act should achieve this three-part assessment to be constitutional. The absence of judicial or legislative supervision over the executive's policymaking under Section 69(1) makes it a disproportionate restriction on a person's essential right to privacy and, consequently, undemocratic.

According to another speech by Justice Sikri, "Data can be mined and collated to reveal your choices, preferences and thinking; where it affects the privacy of people, it becomes a dangerous instrument, then it raises issues of dignity".[18]

Entrustment of non-delegable power

The power of attorney authorizes a representative to act on behalf of the principal. In the background of the statement issued by the ministry, the dread is that the power of the capable authority (in this case, the Union home secretary) of surveillance of individuals has been delegated to the government agencies as a substitute of the prearranged policy of giving sanction on a case-by-case basis.

The notification has lost credibility by negating to follow Rule 3, which precedes Rule 4, stating, "directions for interception or monitoring or decryption of any information". It notes, "no person shall carry out the interception or monitoring or decryption of any information" in any computer "except by an order issued by the competent authority". None of the provisions in Rule 3 was followed by the MHA.

[15] Gobind v. State of M.P., (1975) 2 SCC 148
[16]Justice K.S.Puttaswamy(Retd) vs Union Of India WRIT PETITION (CIVIL) NO. 494 OF 2012
[17] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[18]https://www.livelaw.in/top-stories/threat-of-surveillance-bjustice-sikri-142784, 30. Mar.2019

Hence these issues have drawn worldwide attention on this drastic step taken by the MHA and attracted criticism for the same.

Conclusion

Where according to Shantanu Sen, a former CBI joint director, such delegation of authority could be viewed as "making governance simpler"[19], that seeking approval each time through the home secretary could sometimes delay critical interceptions by hours or even days. Another clarification has been provided by the MHA itself, there have been no additional power given to any of the security or law enforcement organisations by the S.O. dated 20.12.2018[20]. It also stated that each and every case of such interception, monitoring, decryption of user data has to be approved by the Union Home secretary[21]. Hence the government has been actively defending its decision which is in public interest and for the greater good accordingly. But the reality stays that now, consumer's data is collected, consumers can be easily tracked, monitored, traced and intercepted through a dictatorial imposition by the Indian government in general and people in authority in particular. The competing need for privacy, data collection and surveillance, in part, lays out the landscape of a technology-led society we are building today[22].

This question of drawing a line from where the governments should not trespass to citizen's personal space has been ignored heavily by the State. The solution to any problem comes after due recognition of the same. Hence, the above notification is an initial threat to the fundamental right to a dignified life since Surveillance nowadays is far more persistent and proficient of violating the privacy of the consumer en masse than it was eighteen years ago. Experience has shown that the judgements upholding right to privacy have not been as effective as they were envisioned to be by the then experts. Hence, even if the notification has been placed for a nobel cause, the focus

[19] Telegraph India, Government surveillance order raises 'power of attorney' question, G.S.Mudur, 23.12.18

[20] Some points on Lawful interception or monitoring or decryption of information through computer resource, 21 DEC 2018 3:23PM by PIB Delhi, www.pib.nic.in/PressReleseDetail.aspx?utm_campaign=fullarticle&utm_medium=referral&PRID=1556945

[21] IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, rule22, (2009)

[22] Ensuring Privacy in a Regime of Surveillance, Mahima Kaul, March 2014,http://www.india-seminar.com/2014/655/655_mahima_kaul.htm

must not skew from the message it is sending to the citizens regarding their safety and security. The positioning of the largest surveillance plans in Indian history requires a fundamental reimagining of a better accomplished and capable Indian surveillance law that protects the right to privacy while fulfilling the national security obligations as well. Such Parliamentary sanction of (and oversight over) the government's surveillance projects is authoritative and undemocratic and must be reviewed before a precedence of arbitrariness is set.

Conclusively, while technological advancements itself is continuously criticized for the failure in the protection of the privacy of the individuals, the fact is that these loopholes come in the system via poorly formed legislations and misdirected agreements between the governments and its subjects. Just as in this case, when notifications are formed without discerning of the people who could have unjustified, illegal and unwarranted access to individual's data, or about how the data could be used and abused despite the reasons illustrated due to the lack of unaccountability, is when the complications really start. What we require however is a stationary set of rules guaranteeing privacy protections, transparency regarding the very intent and exhaustive degree of a project produces liability, control and accountability, despite the volatile leaps in the development of technology to keep the working system of India the epitome of liberalism it claims to be.