Are India's laws on surveillance a threat to privacy?

This article is related to General Studies-Paper II (Governance).

The Hindu

28 Dec., 2018

Yes

Writer - TATHAGATA SATPATHY (Biju Janata Dal MP)

India might soon become a police state with bureaucrats having access to personal information.

Last year, the Supreme Court ruled in a landmark judgment that privacy is a fundamental right. There were celebrations across the nation after this judgment. Sadly, however, the same court completely changed its character a year later in the Aadhaar judgment. It upheld Aadhaar-PAN linkage and allowed the unique number to be used for government schemes and subsidies. Thus, the segment of the population that neither pays tax nor avails of any government subsidy is now left out. After this judgment, the wheels of governance seem to be rolling in a different direction. Apart from passing small but insidious executive orders on a regular basis, both the Central and State governments have now started taking steps to curtail the liberties of citizens.

Denying the right to privacy

The best example of this came to light recently. This month, the Ministry of Home Affairs issued an order granting authority to 10 Central agencies, including the Delhi Commissioner of Police, the Central Bureau of Investigation (CBI), and the Directorate of Revenue Intelligence, to pry on individual computers and their receipts and transmissions "under powers conferred on it by sub-section 1 of Section 69 of the Information Technology Act, 2000 (21 of 2000), read with Rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009". It has authorised these "security and intelligence agencies" to intercept, monitor and decrypt any "information generated, transmitted, received or stored in any computer resource". This is seen as an extreme measure to deny people their right to privacy — more so because agencies such as the Delhi Police, the CBI, and the Directorate of Revenue Intelligence cannot be strictly termed as organisations concerned with homeland security. Internal security is the main excuse being given for issuing such a directive. Given that the Lok Sabha election is to take place next year, the executive order seems to hint at a different game being played.

The sole fascination of this government seems to be collection of data. With an unquenchable thirst for information, the government at the Centre and most governments in the States have set out on a surveillance race. This will be the fastest process to turn India into a police state. While politicians change every five years, the country's governance system is being left at the mercy of bureaucrats. It is this class of people which is pushing the 'police state' agenda. This especially becomes easy when the democratically elected leader starts suspecting every other elected member as well as citizens. Taking advantage of this mindset of paranoia and isolation, underlined with the greed for power, the bureaucrat seems the most trustworthy and harmless. It is obvious that he will not aspire for the ultimate throne that these apex politicians desire. This makes him a non-adversary.

Cloak-and-dagger surveillance

The MHA order that empowers these 10 agencies to do whatever they want makes it clear that panic has set in. This fear is a threat to democracy at large. With this kind of cloak-and-dagger surveillance being encouraged by the system, India might soon end up as a police state with bureaucrats at the lowest level having access to personal information of virtually every citizen.

No

Writer - KARNIKA SETH (cyberlaw expert and advocate in the Supreme Court of India)

In exceptional circumstances, the right to privacy can be superseded to protect national interest.

The Constitution of India guarantees every citizen the right to life and personal liberty under Article 21. The Supreme Court, in Justice K.S. Puttaswamy v. Union of India (2017), ruled that privacy is a fundamental right. But this right is not unbridled or absolute. The Central government, under Section 69 of the Information Technology (IT) Act, 2000, has the power to impose reasonable restrictions on this right and intercept, decrypt or monitor Internet traffic or electronic data whenever there is a threat to national security, national integrity, security of the state, and friendly relations with other countries, or in the interest of public order and decency, or to prevent incitement to commission of an offence.

Right to privacy is not absolute

Only in such exceptional circumstances, however, can an individual's right to privacy be superseded to protect national interest. The Central government passed the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, that allow the Secretary in the Home Ministry/Home Departments to authorise agencies to intercept, decrypt or monitor Internet traffic or electronic data. In emergency situations, such approval can be given by a person not below the Joint Secretary in the Indian government. In today's times, when fake news and illegal activities such as cyber terrorism on the dark web are on the rise, the importance of reserving such powers to conduct surveillance cannot be undermined.

There should be some reasonable basis or some tangible evidence to initiate or seek approval for interception by State authorities. This is the position in the U.S. Any action without such evidence or basis would be struck down by courts as arbitrary, or invasive of one's right to privacy. Therefore, the framework of the prescribed procedure needs to be adhered to, and its implementation needs conformance, both in letter and spirit. Any digression from the ethical and legal parameters set by law would be tantamount to a deliberate invasion of citizens' privacy and make India a surveillance state.

Checks and balances

The government needs to increase accountability and responsibility, and infuse reasonable checks and balances in exercising these surveillance powers. The recent order passed by the Central government is within the ambit of its powers under Section 69 of the IT Act. However, present implementation of the Intermediary Rules of 2011 will have to be tested on the grounds of reasonableness, fairness, proportionality and judicious exercise of powers.

Another important aspect is that an individual may not even know if her electronic communications are being intercepted/monitored. If such surveillance comes within her knowledge, due to the obligation to maintain confidentiality and provisions in the Official Secrets Act, she would not be able to know the reasons for such surveillance. This can make surveillance provisions prone to misuse.

Therefore, the role of the review committee is quite significant: The committee will aid in checking any arbitrariness in the exercise of these powers. Only 10 agencies have been declared as authorised agencies to confer certainty in this regard.

In People's Union for Civil Liberties v. Union of India (1996), the Supreme Court had set rules for the judicious exercise of surveillance and interception in phone tapping cases. The same fundamental principles should hold good in cyberspace too.

It's Complicated

Writer - ANITA GURUMURTHY (With IT for Change, an NGO that works at the intersection of technology and society)

We need to move towards a new legal framework for surveillance.

Over the past decade, we have been witness to many legal, juridical and executive interventions that comprise the highly contentious terrain of surveillance in digital times — from the amendment to Section 69 of the IT Act in 2008 that expanded the government's powers of interception, to the recent Supreme Court order directing the Central government to frame guidelines for social media intermediaries to address sexually abusive content.

The Centre's most recent proposal to amend the Intermediary Rules, 2011, has been justified as necessary to trace the "originator" of "unlawful" information, in the wake of a fake news epidemic. The Government of India has claimed that social media has brought new challenges for law enforcement agencies, including inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, and incitement to violence.

Powers of the state

The regime's moral panic is not all unfounded. It is partly explained by the fact that communication arenas in the digital age are mostly controlled by transnational corporations. Over the last few months, there have been several cases where the police have expressed their inability to trace offenders because intermediaries have refused to cooperate.

Trends in surveillance point to an obvious tension that the scale of communication activity and its private architecture represent for state agencies. To bring justice to victims of online gender-based violence, the police must obviously do what may be necessary to marshal evidence and trace the offender. However, as critics have held, the overly broad contours of the proposed amendment to the Intermediary Rules confer unchecked powers on the executive, reminiscent of the arbitrariness that led to the famous Shreya Singhal case (2015). In the absence of judicial or legislative oversight, such powers result not only in a disproportionate restriction on individual fundamental right to privacy, but also have far-reaching consequences for other freedoms — a chilling effect on the freedom of speech and association and democratic participation. Also, cybersecurity experts caution that it's not possible to create a "back door" decryption to target one individual, and that tampering with encryption can compromise security for all.

Hence, the digital environment requires a rethink on the rule of law, the very basis upon which the logical connection between constitutional principles, legal norms and procedural rules is tied together. We need not debate the whether or why

of surveillance, but the how, when, and what kind of surveillance, moving towards a new legal framework for surveillance.

Test of proportionality

All measures within such a framework must pass the test of proportionality specified by the right to privacy judgment. They must also account for how digital technologies are implicated in the problems of opacity, arbitrariness and impunity that characterise the rules and current practices of surveillance. Intermediaries must be mandated to locate servers in India. The oversight of algorithms, employed by state agencies and corporations, is an important aspect. Rules for digital evidence collection must be specific to technological applications. The U.S. Supreme Court has held that law enforcement officials can make requests for such information only after obtaining a warrant, which requires them to demonstrate probable cause.

The Centre's attempt to tinker with the Intermediary Rules seems to suggest a cart-before-horse approach, with little thinking on how its social and technological fallouts will impede the rights that make a robust democracy.

GS World Team...

Section-69 of the Information Technology Act, 2000

Why in the discussion

- Recently, according to the Home Ministry notification, 10 agencies have been authorized to block, monitor and decrypt any information generated, transmitted, received or stored in any computer resources.
- Under section 69 of the IT Act, 2000, the government can ask any agency to monitor the data.

What is it?

- According to this, if the Central Government feels that any data is needed to maintain the security, integrity, friendly relations with other countries or prevent crime, then it can direct the concerned agency.
- The IT Act was made in 2000. There is a provision in it that if the government wants to protect the security, integrity or patriotism of the nation, it can monitor the computer of any person or organization.
- However, which agencies will be given powers to monitor, it only decides the government. Monitoring any computer or Internet communication is called data interception.

Will only computer be monitored?

- In order, the government has only talked about computer monitoring, but it comes from laptops and desktops to mobile and all digital devices. That's because the government had said in the Parliament saying the definition of a computer was that any electronic, magnetic, optical or other high-speed data processing device that performs logical, semantic, or memory related work is called a computer.

In what forms can our government ask us for data?

- According to this order, the government can do three things. First - intercept or tap
- Second- Monitoring our data and third- decrypting our messages or notifications.

How the privacy with this order is in danger?

- The amount of data we use every day is enough to find out what your behavior is, what your tendency is, what your likes and dislikes are, whose supporters and opponents are you? Overall, your data can be profiled.
- Indeed, small electronic data can be made from different mediums to a 'meta data', which is enough for profiling of any person. Through this profiling, the government can do everything that he wants to do. This is exactly the same way, the way Cambridge Analycia profiled people.

Why protest?

- This order of the government is based on Section-69 (1) of the IT Act, but in August 2017, the Supreme Court had declared privacy as a fundamental right while giving a decision in the Puthaswamy case. The government's order is not only a threat to the fundamental right of privacy but also a violation of the Supreme Court's decision.
- The order of the government is also a violation of Section-69 (1) of the IT Act. Because this section does not give unlimited power to the government to monitor the general public.
- It can only monitor the computer to maintain the integrity or integrity of the public's interest or nation. But the government has not made it clear in its order why and when will they monitor the computer?

Expected Questions (Prelims Exams)

1. Consider the following statements-

   1. Through the section 69 of the IT act, 2000, all central agencies have been provided the power to survillance all the personal computers and their proceeds.
   2. Through the article 21, privacy has been announced as fundamental right.

   Which of the above statements is/are correct?

   (a) Only 1 (b) Only 2

   (c) Both 1 and 2 (d) Neither 1 nor 2

Expected Questions (Mains Exams)

Q. Is Indian law on survillance (Section 69 of the IT act, 2000) is a threat to privacy? Elucidate your suggestions, highlighting its support and opposition. **(250 Words)**

Note: Answer of Prelims Expected Question given on 27 Dec. is 1(c).