On A Shaky Foundation

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

The Hindu

Writer - Siddharth Sonkar, Sayan Bhattacharya (students of the National University of Juridical Sciences)

26 Dec., 2018

"Section 69 of the IT Act allows for disproportionate state action, and is antithetical to the right to privacy."

The Union Home Secretary, last week, promulgated an order authorising 10 Central agencies to monitor, intercept and decrypt information which is transmitted, generated, stored in or received by any computer. Under the order, an individual who fails to assist these government agencies with technical assistance or extend all facilities can face up to seven years of imprisonment or be liable to be fined.

The notification was reportedly issued in pursuance of powers stipulated in Section 69 of the Information Technology Act, 2000, which enables government agencies to intercept personal information of citizens under certain conditions. The Ministry, in response to flak from the Opposition, has issued a clarification that the authorisation is in conformity with the process stipulated in the IT Rules, 2009.

What is missed out

The clarification assumes the legitimacy of Section 69 of the IT Act, the basis on which the IT Rules were framed. The IT Rules in turn form the source of power behind the Ministry of Home Affairs (MHA) notification. On the basis of this assumption, the clarification justifies the notification without examining the validity of its source. All that the MHA clarifies is that since the notification conforms with the IT Rules, there is no reason for eyebrows to be raised. This, argument, however, is fallacious since it fails to take a step back and peruse Section 69 of the IT Act, which after K.S. Puttaswamy v. Union of India — 'the right to privacy case', in 2017 — seems to fail the litmus test of constitutionality. Let us explain how.

Why is Section 69 unconstitutional after K.S. Puttaswamy? The nine-judge bench in K.S. Puttaswamy declared that there is a fundamental right to privacy flowing from inter alia Articles 19 and 21 of the Constitution. In order for a restriction such as Section 69 allowing for interception of personal data on a computer to be constitutionally valid, it would not only have to pursue a legitimate state aim (say, for instance, national security) but also be proportionate, so that there is a rational nexus between the means adopted (i.e., authorisation of interception) and the aim.

Section 69 of the IT Act is so broadly worded that it could enable mass surveillance to achieve relatively far less serious aims such as preventing the incitement of the commission of a cognisable offence. Such surveillance could be justified to achieve relatively far less serious objectives such as a Facebook post expressing dissent against government policy which, in the state's opinion, is offensive. The state, through the powers under Section 69, can therefore justify authorising surveillance, purporting this to be a grave concern. The language of Section 69, therefore, speaks abundantly of doublespeak, allowing for disproportionate state action, antithetical to the right to privacy.

Implications for free speech

Under Section 69, the government can intercept personal information under any of the following conditions: when it is necessary in the interest of Indian sovereignty or integrity; security of the state; friendly relations with foreign states; public order; and for preventing incitement to the commission of any cognisable offence related to these. While the first four feature in Article 19(2) of the Constitution, the last, namely preventing incitement to commission of cognisable offences, is not an enumerated restriction. A restriction in the form of authorised surveillance would not be justified unless it is in order to maintain public order, a reasonable restriction under Article 19(2).

The Supreme Court has repeatedly accepted a hierarchisation between "public order" and law and order; it explains this through concentric circles where law and order represents the larger circle within which the next circle, public order, lies, which in turn contains the smallest circle representing the security of the state — the most grave concern. While public order is characterised by public peace and tranquillity, law and order requires preventing the incitement of an offence.

However, Section 69, as mentioned earlier, allows mass surveillance even when only law and order is affected while public order prevails: merely for precluding the incitement of the commission of an offence.

Such a broadly worded provision can have potential ramifications on free speech. This is because a constant sense of being watched can create a chilling effect on online communication, crippling dissent. As far back as 1962, Justice K. Subba Rao had explained in his powerful dissent how a "shroud of surveillance" maims individual freedom by engendering inhibitions that an individual cannot act as freely as he would want to. Surveillance does not show direct discernible harms as such but rather imposes an oppressive psychological conformism that threatens the very existence of individual

freedom. The Supreme Court reiterated this view in K.S. Puttaswamy.

Section 69, therefore, cannot be regarded as a reasonable restriction on free speech as well. Therefore, a simple law and order requirement is an impermissible restriction to free speech unless public order, a much higher threshold, is threatened.

Another inconsistency

Section 69 also falls short of meeting with the principles of natural justice by failing to accommodate pre-decisional hearings. The Section only makes post-decisional hearings before a review committee possible as a part of its procedure, compelling people to give up their personal information without being given an opportunity to be heard.

To conclude, the MHA notification rests on shaky foundations. While the Supreme Court missed the opportunity to examine the constitutionality of Section 69 of the IT Act, looking at the IT Rules to legitimise the notification seems to put the cart before the horse.

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. Section-69 of the IT Act, 2000 empowers the government to put restriction on the individual information (privacy).
   2. IT act has been introduced after the passing of united Nations Commission of International Trade law by united nations.

   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.1:-The encroachment of the right to privacy and independence according to section-69 of IT act by the present government is justifiable to what extent? Analyse. **(250 Words)**

Note: Answer of Prelims Expected Question given on 25 Dec. is 1(a).