Source : www.thehindu.com Date : 2018-12-28

SNOOPING OR SAVING? ON PROPOSED ONLINE SURVEILLANCE

Relevant for: Indian Polity & Constitution | Topic: Indian Constitution - Features & Significant Provisions related to Fundamental Rights, Directive Principles and Fundamental Duties

Laws seeking to regulate online activity, especially on social media, will have to be tested against two fundamental rights: free speech and privacy. Regulations that abridge these rights tend to operate in both positive and negative ways. For instance, statutory norms relating to data protection are seen as essential to protect citizens from any breach of their informational privacy; but attempts to regulate online content are seen with suspicion. The latter category evokes doubt whether they violate their freedom of expression (as enforcement of such rules may involve blocking websites, disabling accounts, removing content and intercepting communication), and amount to surveillance that breaches privacy. Two official documents, one of them a draft proposal, that seek to introduce changes in the way rules for interception and monitoring of computer-based information are applied have caused a furore. The first was an order authorising 10 agencies under the Centre to implement Section 69(1) of the Information Technology Act, as amended in 2008, which allows interception, monitoring and decryption of information transmitted through or stored in a computer resource. The other is a draft proposing changes to the rules framed in 2011 for “intermediaries” such as Internet and network service providers and cyber-cafes. While the order listing 10 agencies does not introduce any new rule for surveillance, the latter envisages new obligations on service providers.

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

A critical change envisaged is that intermediaries should help identify the ‘originator’ of offending content. Many were alarmed by the possibility for surveillance and monitoring of personal computers that this rule throws up. The government has sought feedback from social media and technology companies, but it appears that even services that bank on end-to-end encryption may be asked to open up a backdoor to identify ‘originators’ of offending material. There is justified concern that attempts are on to expand the scope for surveillance at a time when the government must be looking at ways to implement the Supreme Court’s landmark decision holding that privacy is a fundamental right. Some of these rules, originally framed in 2009, may have to be tested against the privacy case judgment, now that the right has been clearly recognised. It is indeed true that the court has favoured stringent rules to curb online content that promotes child pornography or paedophilia, foments sectarian violence or activates lynch-mobs. While the exercise to regulate online content is necessary, it is important that while framing such rules, a balance is struck between legitimate public interest and individual rights. And it will be salutary if judicial approval is made an essential feature of all interception and monitoring decisions.

The Congress must strengthen its democratic processes while choosing CMs

END