Source : www.thehindu.com Date : 2018-12-25

THE CASE AGAINST SURVEILLANCE

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

Last week, a Ministry of Home Affairs (MHA) notification authorising 10 Central agencies to intercept, monitor, and decrypt online communications and data caused a furore in both Parliament and the wider civil society. The notification was described as an incremental step towards a surveillance state. The government's defence was equally swift: it protested that the notification created no new powers of surveillance. It was only issued under the 2009 Information Technology Rules, sanctioned by the previous United Progressive Alliance government. The 10 agencies had not been given a blank check; rather, specific surveillance requests, the government contended, still had to be authorised by the MHA in accordance with law.

But whatever one makes of the government's defence, the MHA notification lays bare the lopsided character of the surveillance framework in India, and highlights an urgent need for comprehensive reform.

The existing surveillance framework is complex and confusing. Simply put, two statutes control the field: telephone surveillance is sanctioned under the 1885 Telegraph Act (and its rules), while electronic surveillance is authorised under the 2000 Information Technology Act (and its rules). The procedural structure in both cases is broadly similar, and flows from a 1997 Supreme Court judgment: surveillance requests have to be signed off by an official who is at least at the level of a Joint Secretary.

Full text of Union Home Ministry's computer surveillance order

There are three features about the current regime. First, it is bureaucratised. Decisions about surveillance are taken by the executive branch (including the review process), with no parliamentary or judicial supervision; indeed, the fact that an individual will almost never know that she is being surveilled means that finding out about surveillance, and then challenging it before a court, is a near-impossibility.

Second, the surveillance regime is vague and ambiguous. Under Section 69 of the IT Act, the grounds of surveillance have been simply lifted from Article 19(2) of the Constitution, and pasted into the law. They include very wide phrases such as "friendly relations with foreign States" or "sovereignty and integrity of India".

Third, and flowing from the first two features, the regime is opaque. There is almost no information available about the bases on which surveillance decisions are taken, and how the legal standards are applied. Indeed, evidence seems to suggest that there are none: a 2014 RTI request revealed that, on an average, 250 surveillance requests are approved every day. It stands to reason that in a situation like this, approval resembles a rubber stamp more than an independent application of mind.

To arguments such as these, there is a stock response: the right to privacy is not absolute. Surveillance is essential to ensure national security and pre-empt terrorist threats, and it is in the very nature of surveillance that it must take place outside the public eye. Consequently, the regime is justified as it strikes a pragmatic balance between the competing values of privacy and security.

Centre’s surveillance order challenges Supreme Court verdict on privacy: experts

This is a familiar argument, but it must be examined more closely. First, let us clear a basic misconception: it is nobody’s case that privacy is absolute. The staunchest civil rights advocates will not deny that an individual reasonably suspected of planning a terrorist attack should be placed under surveillance. The debate, therefore, is not about ‘whether surveillance at all’, but about ‘how, when, and what kind of surveillance’.

In this context, the evidence demonstrates clearly that a heavily bureaucratised and minimally accountable regime of surveillance does nothing to enhance security, but does have significant privacy costs. For example, while examining the U.S. National Security Agency’s programme of mass surveillance, an American court found that out of more than 50 instances where terrorist attacks had been prevented, not even a single successful pre-emption was based on material collected from the NSA’s surveillance regime. Indeed, such a system often has counterproductive effects: a government that is not checked in any meaningful way will tend to go overboard with surveillance and, in the process, gather so much material that actually vital information can get lost in the noise. In the famous ‘privacy-security trade-off’, therefore, it is exceedingly important to assess the balance on the basis of constitutional principles and fundamental rights, rather than blindly accepting the government’s rhetoric of national security.

After the Supreme Court’s 2017 judgment in K.S. Puttaswamy v. Union of India (‘the right to privacy case’), the constitutional contours within which the questions of ‘how, when, and what kind’ have to be answered have been made clear. Any impingement upon the right to privacy must be proportionate. One of the factors of the proportionality standard is that the government’s action must be the least restrictive method by which a state goal is to be realised. In other words, if the same goal — i.e., protecting national security — can be achieved by a smaller infringement upon fundamental rights, then the government is constitutionally bound to adopt the method that does, indeed, involve minimal infringement.

Under these parameters, there is little doubt that on the three counts described above — its bureaucratic character, its vagueness, and its opacity — the existing surveillance framework is unconstitutional, and must be reconsidered. To start with, it is crucial to acknowledge that every act of surveillance, whether justified or not, involves a serious violation of individual privacy; and further, a system of government surveillance has a chilling effect upon the exercise of rights, across the board, in society. Consequently, given the seriousness of the issue, a surveillance regime cannot have the executive sitting in judgment over the executive: there must be parliamentary oversight over the agencies that conduct surveillance. They cannot simply be authorised to do so through executive notifications. And equally important, all surveillance requests must necessarily go before a judicial authority, which can apply an independent legal mind to the merits of the request, in light of the proportionality standards discussed above.

Second, judicial review will not achieve much if the grounds of surveillance remain as broad and vaguely worded as they presently are. Therefore, every surveillance request must mandatorily specify a probable cause for suspicion, and also set out, in reasonably concrete terms, what it is that the proposed target of surveillance is suspected of doing. As a corollary, evidence obtained through unconstitutional surveillance must be statutorily stipulated to be inadmissible in court.

And last, this too will be insufficient if surveillance requests are unopposed — it will be very difficult for a judge to deny a request that is made behind closed doors, and with only one side presenting a case. There must exist, consequently, a lawyer to present the case on behalf of the target of surveillance — even though, of course, the target herself cannot know of the proceedings.

To implement the suggestions above will require a comprehensive reform of the surveillance framework in India. Such a reform is long overdue. This is also the right time: across the world, there is an increasingly urgent debate about how to protect basic rights against encroachment by an aggressive and intrusive state, which wields the rhetoric of national security like a sword. In India, we have the Supreme Court's privacy judgment, which has taken a firm stand on the side of rights. Citizens' initiatives such as the Indian Privacy Code have also proposed legislative models for surveillance reform. We now need the parliamentary will to take this forward.

Gautam Bhatia is a Delhi-based lawyer. Disclaimer: he assisted in the drafting of the Indian Privacy Code (saveourprivacy.in), a draft data protection law that proposes surveillance reform

END