In Defence of the MHA Surveillance Order, 2018.

DECEMBER 25, 2018

The Ministry of Home Affairs (MHA) (Cyber and Information Security Division) via order dated 20th December, 2018 signed by the Home Secretary Rajiv Gauba gave the power of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer to ten central agencies namely the Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, CBI, National Investigation Agency, Cabinet Secretariat (Research and Analysis Wing), Directorate of Signal Intelligence (in Jammu and Kashmir, North-East and Assam only) and the Delhi Police Commissioner via power conferred to the Central Government by sub-section (1) of section 69 of the Information Technology Act, 2000.

Section 69A of the Information Technology Act, 2000 provides that the Central Government or any of its officers specially authorised in the interest of sovereignty and interest of Bharat, defence of Bharat, security of state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence may direct any agency of the Government to block for access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

Soon after this order was released, all the social media pages were full of criticisms, especially by the opposition, with respect to the above mentioned order and the biggest concern all of them had was their Right to Privacy and the recent 9 Judge bench making the Right to Privacy a part of the fundamental rights conferred to every citizen of Bharat. But the biggest problem with us is that we haven’t read in its entirety what the 9 judge bench has said in their judgement which consists of 547 pages in total. For the same reason we will try to explore few relevant parts of the judgement strictly with respect to the MHA surveillance order.

On 24th August, 2017, the Hon’ble Supreme Court of Bharat in the case of Justice K S Puttaswamy vs. Union of India, decided unanimously by a 9 judge Constitution Bench, the Hon’ble Supreme Court of Bharat held that the Right to Privacy is a fundamental right flowing from the right to life and personal liberty, embodied under Article 21 of the Constitution of Bharat, as well as other fundamental rights securing individual liberty in the Constitution. But just like other fundamental rights, privacy too can be restricted in well-defined circumstances. Even Justice Chandrachud (speaking for Chief Justice Khehar,
Justice Agarwal, Justice Nazeer and himself) in his judgement on paragraph 183 states that like the right to life and liberty, privacy is not absolute. The limitations which operate on the right to life and personal liberty would operate on the right to privacy. Any curtailment or deprivation of that right would have to take place under a regime of law. The procedure established by law must be fair, just and reasonable. The law which provides for the curtailment of the right must also be subject to constitutional safeguards.

Referring to Richard A Posner, an American jurist and a former United States Circuit Judge of the United States Court of Appeal, who in his article “Privacy, Surveillance, and Law” published in The University of Chicago Law Review (2008) stated that “Privacy is the terrorist’s best friend, and the terrorist’s privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defence of national security...”. Posner notes that while “people value their informational privacy”, yet “they surrender it at the drop of a hat” by readily sharing personal data in the course of simple daily transactions.

The paradox, he observes, can be resolved by noting that as long as people do not expect that the details of their health, intimacies and finances among others will be used to harm them in interaction with other people, they are content to reveal those details when they derive benefits from the revelation. As long as intelligence personnel can be trusted to use the knowledge gained only for the defence of the nation, “the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks”. Posner’s formulation would indicate that the State does have a legitimate interest when it monitors the web to secure the nation against cyber-attacks and the activities of terrorists. Relying on the same and for the same reasons Justice Chandrachud in his judgement on paragraph 180 laid down a three-fold requirement which are to apply to all restraints on privacy. The three-fold test is first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.

Justice Chandrachud also noted that apart from national security, the state may have justifiable reasons for storage and interception of data, prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Justice Chandrachud also draws distinction between anonymity and privacy in his judgement and says that Privacy involves hiding information whereas anonymity involves hiding what makes it personal. An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the state may assert a legitimate interest in analysing data borne from hospital records to understand and deal with a public health epidemic such as malaria or dengue to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it.
Not just Section 69 of the Information Technology Act, even sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 provides that on the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised (the 10 agencies in the present case) in this behalf by Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of Bharat, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order. The agencies by order of the Central Government had the power to intercept since the enactment of the Telegraph Act in 1885 but it was only limited to telegraphs since it being the only mode of communication in that era. But clearly the main intention of this Act is to keep a close eye on the offenders and intercept communication if necessary in the interest of sovereignty, security and public order.

Concluding with the golden works of Justice O Chinnappa Reddy from the Malak Singh vs. State of Punjab and Haryana (1981) case where he said that prevention of crime is one of the prime purposes of the constitution of a police force. It is the duty of the police officers to collect and communicate intelligence affecting the public peace, to prevent the commission of offences and public nuisance. In connection with these duties it will be necessary to keep discreet surveillance over bad characters and other potential offenders. Organised crime cannot be successfully fought without close watch of suspects. Thus it is not unlawful for the police to conduct surveillance so long as it was for the purpose of preventing crime and was confined to the limits prescribed by law or is mere a close watch on the movement of a person under surveillance without any illegal interference.

*Arindam Bharadwaj is currently in his 3rd year pursuing BA-LLB (Hons.) from Jindal Global Law School, Sonepat, Haryana.*