Pegasus has given privacy legislation a jab of urgency

Photo: AFP*4 min read .* Updated: 05 Aug 2021, 10:11 PM IST**Abhinav Mehrotra**,**Chhaya Bharadwaj**

Pegasus has shown just how easy it now is for governments to spy on people. Such tools being in wide use has roused calls for legislative action to keep them under democratic supervision

The revelation that global surveillance was carried out on human-rights activists, journalists, lawyers and many others across the world—including in India and other countries like Azerbaijan, Bahrain, Hungary, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the UAE—through Pegasus, a hacking software sold by Israeli surveillance company NSO, has dominated the news. Pegasus is a malware that infects iPhones and Android devices to enable operators of the tool to extract messages, photos and emails, and, among other things, record calls without the phone user knowing. Consequently, a need has widely been felt for legislation to deal with data protection and privacy in India. This issue is especially significant given that in the Justice K.S. Puttaswamy vs Union of India case of 2017, a nine-judge bench of the Supreme Court held the right to privacy to be an intrinsic part of the right to life and personal liberty under Article 21, and as part of the freedoms guaranteed by Part III of the Constitution of India.

Although the Indian government had introduced the Personal Data Protection Bill on 11 December 2019, after having set up a committee of experts under the chairmanship of Justice B.N. Srikrishna in 2017 that was tasked with identifying key data protection issues and ways to address them, it is yet to become law. The bill is a diluted version of what that panel had proposed, as it exempts agencies of the central government from its application and empowers the government to direct data fiduciaries to submit personal as well as non-personal data of Indian citizens to it under Section 91.

This has been at the core of the recent fight between Twitter and the government, as a result of which Twitter lost its liability protection. Interestingly, what constitutes ‘personal data’ is defined under

Section 3(28) of the bill to mean data that directly or indirectly identifies a natural person, or relates to any characteristic, trait or attribute of such a natural person, but there exists no definition for non-personal data.

In practice, the government has enabled the use of various statutory laws to intrude into the privacy of citizens. For example, under Section 5(2) of the Indian Telegraph Act, 1885, the government can intercept a message or class of messages in the interest of India's sovereignty and integrity, security, friendly foreign relations and preventing the incitement of illegal acts. The procedure to do so finds place under Rule 419A of the Indian Telegraphic Rules, 1951.

Coming back to the proposed bill, personal data breaches are addressed under Section 25, which imposes a duty on the data fiduciary to inform the Data Protection Authority of India (DPAI) in case of any breach of personal data that may cause harm to the data principal. The duties of the DPAI have been laid down under Section 41, which are to protect the interests of data principals, prevent any misuse of personal data, ensure compliance and promote awareness about data protection. Despite these safeguards, there exist concerns about the independence of the DPAI. Seen in this light, inspiration could be drawn from the European Union's Model Regulation known as the General Data Protection Regime (GDPR). As per its Article 34, it is the duty of the controller to convey information on a data breach to the data principal in case it is likely to result in significant risk to the rights and freedoms of the concerned person.

From an international perspective, a a Pegasus-like revelation occurred in the US in 2013, when it emerged that its National Security Agency had conducted surveillance of millions of Americans' telephones. The revelation was made by a current political asylee, Edward Snowden. He also brought to light that through a program called PRISM, the US government was monitoring emails and social media posts of millions of Americans and non-Americans, including through Facebook, Yahoo and Google. Under the 50 U.S. Code § 1861, the US government can access records, including telephones, for foreign intelligence and international terrorism investigations. When the 2013 act of phone-tapping by the administration was challenged in court, the US government invoked this law. However, the Federal Court of Appeals finally ruled that the government's action which led to millions of people being spied upon exceeded its authority under the law. It was after this judgement that the government passed the USA Freedom Act of 2015 to reform its procedures to conduct surveillance, trap and trace devices, and use other forms of information to gather foreign intelligence, take counter-terrorism measures, etc. This law also prohibits bulk collection of information and ensures transparency.

It is fair to conclude that with advancing technology, the ability of governments and private actors to peek into the private lives of individuals has expanded. Additionally, on the pretext of terrorism and national security, governments around the world have blurred the lines of reasonable surveillance and data collection. In the larger scheme of things, states need to adopt national laws that not only deal with data protection and privacy, but also educate people of risks related to identity theft and

fraud in the digital world. Such laws should also lay down proper processes for the collection of private information and require privacy safeguards encoded into tools of technology.

Abhinav Mehrotra & Chhaya Bharadwaj are lecturers at OP Jindal Global University, Sonipat